ESD-TR-77-24

COMPUTER SECURITY REQUIREMENTS: AN INVESTIGATION OF COMPUTER SECURITY COSTS

James P. Anderson Company
Box 42
Fort Washington, PA 19034

January 1976

Approved for Public Release; Distribution Unlimited.

Prepared for

DEPUTY FOR COMMAND AND MANAGEMENT SYSTEMS
ELECTRONIC SYSTEMS DIVISION
HANSCOM AIR FORCE BASE, MA 01731

LEGAL NOTICE

When U.S. Government drawings, specifications or other data are used for any purpose other than a definitely related government procurement operation, the government thereby incurs no responsibility nor any obligation whatsoever; and the fact that the government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data is not to be regarded by implication or otherwise as in any manner licensing the holder or any other person or conveying any rights or permission to manufacture, use, or sell any patented invention that may in any way be related thereto.

OTHER NOTICES

Do not return this copy. Retain or destroy.

This technical report has been reviewed and is approved for publication.

Donald P. Eriksen
DONALD P. ERIKSEN
ADP System Security Projects Manager

Roger R. Schell
ROGER R. SCHELL, Lt Colonel, USAF
ADP System Security Program Manager

FOR THE COMMANDER

Frank J. Emma
FRANK J. EMMA, Colonel, USAF
Director, Computer Systems Engineering
Deputy for Command & Management Systems

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER ESD-TR-77-24	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) COMPUTER SECURITY REQUIREMENTS: AN INVESTIGATION OF COMPUTER SECURITY COSTS		5. TYPE OF REPORT & PERIOD COVERED Task Report 1975
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) James P. Anderson		8. CONTRACT OR GRANT NUMBER(s) F19628-72-C-0198
9. PERFORMING ORGANIZATION NAME AND ADDRESS James P. Anderson Company Box 42 Fort Washington, PA 19034		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS PE 64708F Project 6917
11. CONTROLLING OFFICE NAME AND ADDRESS Deputy for Command and Management Systems Electronic Systems Division Hanscom AFB, MA 01731		12. REPORT DATE January 1976
		13. NUMBER OF PAGES 77
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)		15. SECURITY CLASS. (of this report) UNCLASSIFIED
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE N/A

16. DISTRIBUTION STATEMENT (of this Report)

Approved for Public Release; Distribution Unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Computer Security
Computer Security Costs
Security Problem Avoidance Techniques

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

A study of the costs associated with the three most popular security problem avoidance techniques provides a lower bound estimate of $3 million per year saving by applying technology. The cost savings estimated appear conservative because of the difficulty in quantifying costs of avoidance methods, and the omission of any consideration of costs of 'mission essential' functions now being performed in isolation due to security constraints or requirements.

(continued on reverse)

Item 20. Continued.

Of the several approaches being taken to provide security, controlled sharing and VMM systems (to provide isolation) will reduce costs projected from current estimates significantly. Of the two approaches, the controlled sharing development appears to have maximum beneficial impact because it is applicable without change in virtually all application areas.

Table of Contents

Table of Contents (Continued)

List of Tables

List of Tables (Continued)

List of Figures

1. INTRODUCTION AND BACKGROUND

1.1 INTRODUCTION

This report attempts to provide a basis for quantifying current and projected costs of USAF (military) computer security practices and the impact of various technological developments that will become available in the next five years.

Earlier estimates of USAF computer security costs (AND 72) were made by allocating a percentage of the total USAF ADP expenditures including personnel, equipment, site preparation, communications, etc. The value of that estimate has been questioned because it is based only in part on hard data.

After reviewing the availability of data that could be used in determining costs of computer security, it was concluded that it would be impossible to obtain comprehensive cost data for every item that might contribute to computer security costs. (As examples: the annual costs of guard forces required to physically protect a computer site, the on-going costs of administrating clearances and lists of authorized users, etc.)

A major element of computer security costs can be directly related to the number of computer systems and central processing units (CPUs) in use, and this data is available. As a result, it was decided to base the study on this available data fully recognizing that some cost factors would not be included. In spite of this, it is believed that the study is useful in providing a realistic lower bound on computer security costs.

The analysis will attempt to put into perspective the various factors entering into the costs associated with any particular alternative. Essentially, it takes into account the uneven development of ADP practices in the Air Force and recognizes that due to the relatively simple level of some processing being performed in some installations, that their current and near-term security needs are met by quite simple security methods. While simple methods may in many instances be acceptable today, it is not clear that they will remain so in the future. The trend to more on-line integrated networks of computers noted in (SAD, 74) is real, and obsoletes the traditional (simple) protection mechanisms from the beginning. While there has been increased interest in determining costs of following (or not following) various security development policies, to date, there has been no methodology applicable to military systems.

A recent PhD thesis by Goldstein (GOL 75) has developed a cost model for implementing privacy controls. The methodology used in that analysis develops costs of personnel (in categories of programmer, executive, clerical, auditing), cost of capital and costs of hardware (storage and processing elements).

Goldstein was attempting to assess the impact in the civilian section of various requirements of the (then proposed) privacy legislation on on-going data processing operations that did not have to meet any of the requirements previously. Secondly, the requirements studied by Goldstein included a variety of items important to 'privacy', but not security such as notification to data subjects of the existence of records on them; handling inquiries (existence, accuracy) regarding records, employee training, consent to transfer data and the like. Only the costs of physical security could be considered relevant to the intent of this study. Goldstein's study is not especially useful even in regard to physical security because it assumes that there was no physical security before and provides no standards on which to relate the estimated one-time costs for securing a site. His on-going costs for physical security are primarily those associated with a guard force.

1.2 SECURITY THREAT

This study is based on two premises; that there exists a class of data that requires protection, and that there exists a threat of clandestine[1] operations against the Air Force for the purpose of acquiring such data in connection with espionage required to support war plans, or for the purpose of corrupting the data to cause a pin-down[2] of some part of the USAF operational resources.

The data requiring protection is that data classified in accordance with DoD 5200.1 and AFR 205-1; (commonly called classified data).

In general, the analysis is based on an understanding of the technical vulnerabilities of modern computing systems and the limitations on operating flexibility that the vulnerabilities impose rather than the measured extent to which an actual enemy threat exists. Thus, the analysis is based on the manner in which computer systems are used to overcome or minimize the effect of technical vulnerabilities rather than on current intelligence estimates which are ephemeral.

[1] activities sponsored or conducted by a nation against another nation using secret or illicit means (AFR 205-1)

[2] activities which will result in a system's incapability to function for a period sufficiently long enough to insure its destruction

2. ORIGINS OF THE SECURITY 'PROBLEM'

2.1 SOURCE OF SECURITY REQUIREMENTS

The security 'problem' for USAF (and DoD) computer systems derives from operational requirements which determines the uses of computers. The main operational components contributing to the security 'problem' are the requirement to share hardware, and the requirement to share data. These two operational requirements and the fact that currently available computer systems do not have effective internal controls sufficient to protect classified data from unauthorized access by users of the systems are the setting for the 'security problem.'

Under these circumstances, only if all data is at a single classification level and/or all users of the system have clearances greater than or equal to the highest classification of the data, are there no computer security problems, only physical and administrative security problems that are generally well understood and (more or less) easily solved.

Currently the state-of-the-art supports two approaches to handling computer security problems. First, it provides techniques for avoiding the computer security problem. These techniques developed over the past 25 years include dedicated computer systems; operating computers at a 'systems high' level with all users having a clearance at the level of the highest classified data processed by the system and the like. Secondly, ad hoc security 'features' or 'enhancements' are available on most manufacturers equipment. The enhancements and features most frequently provide control of access to the systems, or to system applications. The features and enhancements may nominally permit some sharing, but their effectiveness is not assured. The limited technical approaches to solving the computer security problems (such as virtual machine systems) provide only limited sharing, may require expensive restructuring of programs and carry significant operating overhead penalties.

An important impact of not having internal computer security controls is economic. All of the methods for avoidance of security problems carry heavy cost penalties both for procurement and for subsequent operations and maintenance of the systems. Alternate forms of delivery of a needed operational capability that control or bypass the security problems also carry heavy cost penalties.

Lack of adequate internal security controls in computers has a negative impact on how systems are used. Typical qualitative effects are inefficiencies due to maintaining redundant files because of classification of some data; or the need to schedule (and reschedule) use of a system in order to use a system at a single classification level (at a time). In addition, lack of adequate internal security controls increases the costs of programming because of the need to compensate for the lack of internal controls. It is noted that some of the procurements planned for the next five years are presumed to have the internal controls necessary and sufficient to solve the security problem. It can be stated categorically that it is not evident that any of the manufacturers are independently pursuing programs to provide the internal controls of the form needed for the solution of the DoD security problems.

2.2 SHARED HARDWARE CONSIDERATIONS

The shared hardware requirement is not a requirement of the function(s) to be performed by a system; rather it is an economic constraint on how data processing is delivered to a set of users. Basically, shared hardware arises from the need or desire to get the maximum utilization of a complex set of hardware through time-division-multiplexing of CPU's and I/O channels and devices using the technique of multi-programming. In some of the more advanced uses of shared hardware, the basic workload is event-driven and cannot be scheduled. (An example is the Military Airlift Command; MAIRS air movement reports system.) As events occur to which users of the system must respond, the programs and data bases used in effecting the response must be immediately available for use. This generally means on-line, awaiting activation.

In the case of shared hardware, there is no logical relationship between the programs and data involved in one job, and the programs and data for another. The co-residence of the jobs is coincidental and not an integral requirement for operating. Except for whatever priorities that arise due to requirements for effecting control of military forces, the data processing requirements of the users of shared hardware can be met with varying degrees of simplicity.

The risks of sharing hardware alone are the same risks associated with the sharing of data; that the internal controls provided by the operating system are not sufficient to assure isolation of one user from another. The consequences of not being able to demonstrate such adequate controls is that the sharing of hardware is constrained. Whether or not this is more than an inconvenience depends on the nature of the installation.

In general, the constraint means the hardware is serially reusable by different clearance levels after an appropriate process of "sanitization" takes place. Other methods available for sharing hardware are discussed below.

2.3 COSTS ASSOCIATED WITH SECURITY PROBLEMS OF SHARED HARDWARE

The case of shared hardware presents an interesting conundrum. The impetus for sharing hardware is clearly economic. The cost of a single system capable of processing the workload of N separate systems is much less than N times the cost of one of the smaller capacity systems. This accepted 'truth' has been formalized into 'Groch's law" which states that the ratio of the (computing) power (i. e. their 'capacity' in some sense) of two computers is approximately equal to the ratio of their sell price squared.

Thus, $\frac{P_A}{P_B} \approx \frac{C_A^2}{C_B^2}$, where P is a measure of power and C is cost.

If one always compares machines to some standard base machine (undefined), then

$$P_A = KC_A^2; \text{ where } K = \frac{P_S}{C_S^2} \text{ , a proportionality constant.}$$

In an empirical study that covers computers available through 1968, Dr. Kenneth E. Knight (KNI 66, KNI 68) found that the conventional expression of Groch's law is very conservative and that one could use:

$$P = K(C)^{2.5} \text{ for scientific systems and}$$

$$P = K(C)^{3.1} \text{ for commercial systems.}$$

What this demonstrates is that there is a sound economic basis for the notion of acquiring high capacity systems and sharing the hardware among several users.

For many users, if not most — the economic benefits are sufficient reason for sharing hardware. Such sharing is economic as long as there are no artificial conditions imposed.

If the hardware must be shared among groups of users of different clearance levels, then the costs of operating shared hardware are increased by the time needed to 'sanitize' a system preparing it for use by lower cleared users. There is also a 'lost opportunity' cost that cannot be easily measured that is associated with not being able to use a computer outside of scheduled times. These increased costs erode the cost benefit ratio that was sought by hardware sharing in the first place. Depending on the options available, and to some extent the environment in which sharing is to take place, the security related costs of operating shared hardware can increase until it is no longer justified to share the hardware, and separate machines are obtained to satisfy the security requirements.

2.4 SHARED DATA CONSIDERATIONS

Of rapidly increasing significance in terms of the number of installations/sites involved is the operational requirement to share data. Unlike shared hardware, whose operational origins arise in the need to perform data processing on demand, and whose justification is given in terms of economics, the requirement for shared data comes about due to the increasing interdependence of military functions, and the integration of appropriate military components into more mission oriented commands

(e. g. Unified and Specified commands), and the need to rapidly restructure military organization to meet specific and often immediate problems in the conduct of military operations. In this kind of environment, the "local" data maintained by individual subordinate commanders on material and personnel readiness, logistics, etc., is of vital importance to both superior commands, and in some instances to equal level lateral commands. Regardless of the reasons, the requirements for sharing data have increased significantly over the past 10 years, especially in the Command and Control area (e.g. World Wide Military Command and Control System, WWMCCS).

Although initial data sharing is taking place between groups of homogeneously cleared users, there are already instances where the data sharing requirement involves classified and unclassified data as well as cleared and uncleared users. (As an example, see the MAIRS system of the Military Airlift Command (MAC.))

Simple isolation techniques are a conceptual approach only suitable for solving the problem of shared hardware. The data and program sharing requirement involves a more complex and intimate access capability than that required for hardware sharing.

The primary aspect of shared data is that there is a logical relationship between the program and data involved in one job, and the programs and data involved in another.

In order to provide for sharing of data (and in general, programs) between dissimilarly cleared users, it is necessary to show that the logical internal controls built in a system are sufficient to contain the lesser cleared user regardless of what 'malicious' actions he may attempt to take against the system using his (authorized) user capabilities.

Note that this requirement is more severe than that for simple hardware sharing because of the numerous internal interfaces that must exist to permit communication between programs about the data (and other programs) being shared. Thus, it is necessary to maintain a general capability for isolation between programs, yet permit (controlled) openings in the isolation to communicate between programs about shared resources and to provide non-scheduled sharing of the resource directly.

Because data sharing is an emerging problem, the costs associated with its solution (or lack of it) are mostly future costs. It is noted that in the anticipated Support of Air Force ADP Requirements through the 1980's (SADPR 85) procurement, the technical solution to the security problem of sharing data among dissimilarly cleared individuals is a requirement.

Technical approaches to providing security for sharing classified data involves providing a logical mechanism to recognize (in a computer) the classification of data (programs, files, etc.), and compare the classification to the clearance of the user (program) attempting the access (for each access) in order to determine whether the attempted access is authorized. This logical mechanism is known as a reference monitor. In addition, secure sharing of classified data requires the ability to isolate the reference monitor function from all users, and each user from all others. While the ability to provide isolation is an integral part of data sharing, it is of itself insufficient to provide the capability needed.

The "spontaneous" development of protection mechanisms on the part of manufacturers has thus far resulted in mechanisms, that even if implemented correctly, will provide limited (non-formal) need-to-know controls, and some effective <u>system</u> access controls, e.g. log-on passwords. These controls are <u>not</u> sufficient in themselves in building a logical internal security system such as is needed to process classified information.

2.5 IMPACT ON FUTURE SYSTEMS

The cost impact on future systems of <u>not</u> pursuing the development of certifiable internal controls can rapidly disappear in a fog of generalities about reduced 'capability' (how measured?), lowered 'operational effectiveness', and the like. While it is evident that such impacts will undoubtedly be felt, it is less evident how it can be measured.

For the near future (5-10 years), it is possible to assess the economic (but not operational) impact by evaluating the incremental costs due to avoidance of security problems and costs associated with various technical approaches now being pursued.

2.6 TECHNICAL APPROACHES TO COMPUTER SECURITY

As noted above, there are basically two approaches to computer security; problem avoidance and problem solution. Among the former techniques are included dedicated systems, "system high" operation, periods processing (scheduled operations) and the like. Among the latter are virtual machine monitor (VMM) designs, attempted retrofit of existing systems, high "integrity" systems, and certified systems.

2.7 PROBLEM AVOIDANCE TECHNIQUES

There are basically three security problem avoidance techniques in use today. These are discussed below, along with their limitations.

2.7.1 Dedicated Systems

This technique of avoidance of computer security problems merely collects all classified processing of a single level in (on) one machine, and all other processing in one or more other systems. The most common application of this avoidance technique is in connection with (compartmented) intelligence support systems co-located with the command and control centers they are supporting. It may well be that the command and control application and the intelligence support system require the computing capability of separate machines; however, such requirements are currently never decided on their functional merits, but are driven by the security requirements.

The disadvantage of the dedicated system technique is that it is a mechanism for sharing of hardware. It does nothing for sharing data (except among like-cleared users).

2.7.2 System High Operation

This technique avoids computer security problems by defining them out of existence. The computer system is operated as though all programs and data were of the same highest clearance. All users of the system are cleared to this level and given an implicit need-to-know, and voila ! — no computer security problems. Since in most instances where this technique is used, processing at the highest classification is rare, the bulk of the work load is of lower classification down to and including Unclassified. Security proprieties are met by placing banner sheets on output warning that the data was processed on a system operating at the "X" level, and that the printout should be reviewed by the user and a determination made of the actual classification. This avoidance technique is quite effective as long as the people who have to be cleared to 'system high' are not too numerous, (the probability of at least one 'malicious' user increases as the number of users increase) and the cost of such clearances can be submerged in the general site administrative costs.

2.7.3 Scheduled Operations (Periods Processing)

This technique avoids computer security problems by scheduling use of a system among users on the basis of the clearance of the users and the classification of the jobs. In effect, it allocates a consecutive portion of the available time to unclassified processing followed by a portion for secret processing, etc. Each allocated portion (period) is dedicated to processing at a single classification/clearance level only. On changing from one level to another, the computer system must be essentially restarted, with a fresh copy of the operating system, and only data and program files of the new classification level. (This change of level is referred to as a 'color change'.)

As a technique, scheduled processing is relatively easy to implement. Its major drawback is the time it takes to dismount the media containing the 'environment' at one classification level, and mount media containing the new level. Further, as a technique it only permits serially reusable hardware sharing.

A variation of this technique, called Job Stream Separator (JSS) (SCH 75) is designed to automate the changeover process (from one classification level to another). JSS also can provide a means of accumulating jobs from remote terminals, running them together in classification batches. JSS is usually thought of in terms of a mini computer acting as a controller, with access to the real memory of the controlled system. Its major advantage is that it can (most reliably) control the transfer of 'environments' between a JSS-local storage to the controlled system. It's major disadvantage is the cost of hardware, and the time it takes to copy the entire environment from one medium to another.

2.8 PROBLEM SOLUTIONS

There are basically only two viable approaches to solutions of the computer security problem(s). These are to provide logical controls for hardware sharing, and logical controls for data sharing. The former includes VMM, and mini-computer networks. The latter includes the security kernel work, capability systems and 'features.'

2.8.1 Virtual Machine Monitors

The virtual machine monitor (VMM) is an attractive approach to the sharing of hardware. A number of papers have been written describing its objective(s) and mechanisms, and several systems have been built and operated (POP 74). The basic technique is to design and implement a simple operating system that uses the technique of multiprogramming to make available to each user an interface to the computer that is functionally equivalent to a complete "raw" or "bare" machine in which there are no restrictions on the type or category of instructions that can be executed. In effect, each user has his own independent machine with no restrictions on how he can use it.

The operating system that creates this environment is known as the virtual machine monitor (VMM) and consists primarily of programs that provide interpretive execution of privileged instructions that are trapped to it and programs that control the time-multiplexing of the real machine to give the effect of many virtual machines. In addition, a major portion of VMM is devoted to interpreting I/O (for integrity and correct operation in/on a VM) and simulating to the user machine controls such as interrupts, error indications and the like.

The security of the VMM rests in the fact that each user has a functionally complete machine of his own in which it doesn't matter whether the instructions being executed are privileged or not. In such a case, the lack of internal controls is of considerably less security importance since in the extreme, each user can be supplied with his own copy of the operating system. The VMM approach attempts to isolate users, one from another and provides a flexible framework for secure hardware sharing. The major disadvantage to a VMM is that secure data sharing (of any kind) must be done externally. Such sharing is at least inefficient and may be ineffective. Since VMMs are just a form of operating system, they have security problems similar to those for ordinary operating systems in that it may be possible to penetrate the VMM to destroy the effectiveness of the isolation (ATT, 1976).

2.8.2 Certifiably Secure Systems

Certifiably Secure Systems have as their objective demonstrably secure data sharing. These developments include, as an integral part of secure data sharing, the ability to share hardware securely as well. As a consequence, it is a general solution to the security problems that arise from sharing of any computer resource.

The approach to obtaining certifiably secure systems requires a formal definition of what secure data sharing means, including definitions of what data or programs are being protected, what the protection encompasses, and how the computer will be able to recognize data requiring protection.

The general schema for producing a formal security system is described in (BUR 74). Briefly, it involves the concept that in a computer there exists a single centralized mechanism that validates the access rights of a process on each and every attempt to reference any object (data, program, device, etc.); that the mechanism is protected from alteration or tampering by the rest of the system's users; and that it is small enough to be formally proven correct (AND 72). This mechanism is referred to as a reference monitor.

The certifiable system appears to offer the best general solution to the sharing problem for any future procurements. It can be used to control sharing of programs and data or as a virtual system effecting hardware sharing.

2.8.3 Capability Systems

Another approach to obtaining secure data sharing is pursued under the name 'capability system.' Essentially, the capability systems permit the owner of an object (program, data set, etc.) to pass a key (the 'capability') to another user if the owner wants the second party to use/or share) the object. The internal mechanisms that support such a design approach are similar to those needed for certifiably secure systems. Nevertheless, the capability systems appear to be suitable for easily implementing a discretionary (i.e. one where each user decides for himself with whom he shares objects under his control) security policy only. Such discretionary sharing is not adequate for DoD needs because it relies on each user doing the right thing about granting access to classified information in his possession. In effect, each user would have to be trusted to follow the rules of handling classified data correctly. The actual U.S. government classification system is more authoritarian (and less trusting) than that. More recently, it has been shown that it is possible conceptually to build a certifiable system using capabilities. Such a system severely restricts what capabilities were intended for, and makes it necessary to prove the correct design and implementation of the entire operating system. Because they are at an early stage of development, capability systems are not considered further.

2.8.4 Security 'Features'

The main difference between the formally specified systems and systems with 'security features' lies in the completeness and effectiveness of the controls provided. The formally specified system is based on a precise (mathematical) definition of 'security' drawn from a model of the DoD security systems. The formal system relates the design elements used to specific parts of the formal definition (e.g. security, rules that must be followed in manupulating various program and data objects in an application). The 'features' approach on the other hand, represents the best intuitive approach on the part of designers to overcome known weaknesses in existing systems. Because 'features' are informal (ad hoc), there is no way to assure their relevance to security in a system, or their 'completeness' (in a mathematical sense).

In systems with security 'features', it appears that the features are there to be used if a user decides to protect some data (discretionary security policy). The kind of sharing evisioned by the designers of the 'features' is pre-planned and generally limited by the ability of a user to remember passwords, (a favorite device to authorize sharing). The 'features' approach has no easy way of recognizing a global authorization (e.g. Secret Clearance) and applying it to all objects under its control. Whether or not this is a fatal liability in any specific instance depends almost entirely on the environment in which the systems are to be used and the type of processing to be done. In general, the more sharing of programs and data is an objective of the system, the weaker the 'features' control of authorization and access becomes.

3. METHODOLOGY FOR EVALUATING SECURITY COSTS

3.1 INTRODUCTION

In general, the method followed for evaluating security costs is to identify for each of the alternative security techniques, the important elements of cost associated with using the technique. The costs are given in terms of the base cost of a computer or system to which the technique is applied. In applying this method it is necessary to determine the number and costs of each computer or system which is the subject of one of the avoidance or solution techniques discussed. This section is merely concerned with development of the methodology. An analysis for USAF systems is presented in Section 4. The following sections individually address each of the six major classes of alternative security techniques: dedicated processing, system high operations, periods processing, job stream separators, virtual machines, and certifiable systems.

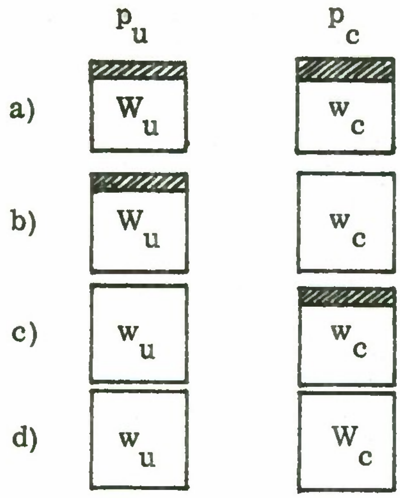
3.2 DEDICATED PROCESSING

Dedicated processing involves using a separate computer system for classified processing regardless of the actual work requirement of the installation. In order to understand what is involved, a formal definition of dedicated processing will be given.

First, a total installation workload, W is defined consisting of two parts; classified work, w_c and unclassified work, w_u. It is <u>assumed</u> that there exists a processing capability (capacity) P involving shared hardware such that

$W \leq P$ (That is, the total installation workload could be supported on an integrated shared hardware base except for security considerations.)

There are four cases of interest shown below:



in the first three cases, $p_u + p_c$ is greater than the actual processing capacity needed, only in the last case are the two processors fully utilized.

A dedicated processing system is said to exist if there exists individual (separate) systems with a processing capability p such that

$$w_c \leq p_c \quad \text{and}$$

$$w_u \leq p_u$$

and $$p_u + p_c < P$$

The problem with this formal definition is the difficulty in measuring **W** and P for most installations. (i.e. covering such cases as $w_u = p_u$, $w_c < p_c$ where $p_u + p_c < P$). Excess processing capacity includes processing elements and peripheral devices (required because components exist only in integral units) as well as excess primary and secondary storage required because of duplicate copies of programs and data at each level.

What we are interested in, ultimately, is the cost of the fraction of extra (unneeded) processing capacity involved in segregating classified from unclassified processing.

Letting $p_u + p_c = P_a$ (actual capacity)

and $P_t = P$ (theoretical capacity)

Then $1 - \frac{P_a - P_t}{P_a} = F$ is the fraction of capacity not actually needed.

In some systems, where P_a is nearly equal to P_t the fraction will be small; in others, where P_a is much larger than P_t, the fraction will be much larger. In general, it would be expected that the distribution of this fraction is over the range 0 to 50%, (i.e., it is expected that virtually no installations will have in excess of 50% over-capacity due to security avoidance and most will be less). There is no data available to support this estimate. It is only proposed as a 'reasonable' estimate, and remains to be validated.

For the purpose of this study, we will use a figure of 25% as the average fraction of over-capacity due to the security avoidance technique of dedicated processing where it is the primary security avoidance method. (This implies that the real value is between 0 and 50%, and the average of 25% will be satisfactory for this estimate.)

The cost of the over-capacity is directly proportional to the total cost of the system. Since we are interested in the macro economic effects of various security avoidance methods, any errors in the basis for this estimate are expected to cancel over any reasonable number of systems.

In general, it is expected that a system of capacity P can be obtained from any manufacturer especially since nearly all manufacturers provide the capability to configure multi-processor systems, and most support multi-processing with their software.

3.3 SYSTEM HIGH OPERATION(S)

Costs associated with System High operations are attributable to the direct costs associated with obtaining clearances to the level necessary.

Let N = number of users of a system
Let M = number initially cleared to highest level
then $(N-M)$ = number requiring clearances
Let C = cost of obtaining one clearance ($300 - $1,000 or higher)
Let Q = retirement (replacement) rate of users

Then initial cost is $(N-M) \times C$ dollars and annual replacement cost is $QN \times C$ per installation.

The latter figure assumes (lacking any detailed information) that replacements will already have clearances in proportion to those that existed among the personnel in the initial application of the technique.

A significant cost which is not quantified nor included in this study is the cost to manually review and downgrade information that is in fact at a level less than system high.

3.4 SCHEDULED OPERATIONS (PERIODS PROCESSING)

The primary cost of scheduled operations is the time (capacity) lost due to changing classification levels. The cost of change over can be developed as follows:

Let U = total time utilized for work; no change of level
Let t = time to effect 1 change of level
Let N = number of changes per day (generally 2; one up, one back)
Let C = cost of equipment

then

available time = $U - Nt$

The percent reduction in effective utilization $= 1 - \frac{U - Nt}{U}$, and the cost of reduced utilization is $C\left(1 - \frac{U \;- N}{U}\right)$

This can also be likened to a hidden <u>increase</u> in dollar cost of a system, and is so treated.

3.5 JOB STREAM SEPARATOR (JSS)

The costs of this technique are akin to the periods processing costs. However, there are additional development and equipment costs associated with this approach.

Let D = development cost of JSS

Let E = per-system special equipment costs

Let I = number of systems where JSS would be applied

then $\frac{D}{I}$ = apportioned development cost

Let U = total time utilized for work; no change of levels

Let t = time to effect 1 level change with JSS

Let N = number of changes/period U

Let C = cost of main equipment.

then % reduction in effective utilization of a system $= 1 - \frac{U - Nt}{U}$

Cost of JSS approach:

$$I \times E + \frac{D}{I} + \left(1 - \frac{(U - Nt)}{U}\right) C$$

3.6 VM APPROACH

The cost of a secure VM system is the development cost of the initial secure VMM for a given system (e.g. a VMM for IBM 370/158; or VMM for HIS 6000 systems) amortized over the number of systems to which it is applied, and the cost of hardware modifications to condition a system for VMM operation. The cost of hardware modifications is not known precisely. Estimates based on several current systems range from 5 to 10% of the base cost of a system. This cost is for hardware retrofit. Whether there will be any significant cost charge as the hardware features needed to support VMM development are designed into new systems remains to be seen.

An expression of VMM cost is given below:

Let D = development cost for a VMM

Let I = number of systems which can support VMM operation

then $\frac{D}{I}$ = apportioned development cost

Let E = per system hardware modification cost (fix-kit)

Let C = cost of equipment

Let OH = % of a system capacity devoted to overhead in controlling VM's

then the per-system cost of the VM approach

$$= \quad E + \frac{D}{I} + OH \times (C + E)$$

3.7 CERTIFIABLE SYSTEMS

The costs of certifiable are the development costs, and the overhead of operating the secure system. While it is expected that there would be some modification of system architecture (in some equipments) to achieve a suitable base for certifiable systems, it is difficult at best to identify the cost of this change because the architecture changes are not exclusively for security reasons but are generally designed to yield direct benefits of other kinds. Under any circumstance it is expected that hardware costs for certifiable systems will be considerably less than 15% of the cost of a system which is not conditioned for certifiable systems.

Let D = development costs

Let I = number of systems over which development is applied

Let C = cost of a system without certifiable system conditioning

Let OH = % of capacity of a system devoted to security overhead

Then the per-system cost of a certified system will be

$$\frac{D}{I} + .15C + OH(1.15C)$$

4. APPLICATION OF METHODOLOGY TO USAF COMPUTER SYSTEMS

4.1 INTRODUCTION

In an attempt to obtain a better estimate of costs of computer security, the methodology of Section 3 was applied to USAF computer holdings.

The USAF was chosen as the subject of the methodology because the USAF is a major user of computers. Its use includes supporting command and control, and communications (CCIP85), and general management functions (CCI 72); the USAF has taken a lead in development of certifiable secure systems, and the results of this analysis are relevant to that program; and to provide baseline costs in an area of surprising complexity.

The only readily available cost data on computers is that in "Inventory of Automatic Data Processing Equipment in the United States Government for Fiscal Year 1974" (INV 74). This particular work is published annually by GSA as a result of a requirement of PL89-306 (Brooks Bill). For a discussion of it as a data source, see (FIS 74).

The Inventory contains data on two kinds of systems; General Management Classification (GMC) and Special Management Classification (SMC). The former are pretty much what one would expect from the name. The latter include control systems, mobile systems (mounted in ships, aircraft or vans) and classified systems whose physical location is classified. The SMC presents such a mixed bag, it was decided to be conservative and consider only the GMC systems. In addition, GMC systems are more of the kind to be shared, or on which data sharing would more likely take place. One generally expects to find control systems in a single classification environment or performing a function that does not produce classified data (although the function itself may require protection).[1]

[1] While some fraction of the SMC systems could have been included in the analysis, there is no consistent basis for selecting either the systems or the fraction. As a result, the analysis is applied to fewer systems than are believed to be affected by security considerations.

Having decided to concentrate on GMC systems, these were examined, and found to include both owned and leased systems, as well as a variety of small systems such as PDP 11's and Burroughs 263's.

4.2 STANDARDIZING THE DATA

In 1974 the USAF had 1577 CPU's (1247 owned (73%) and 330 leased (26%)) in 1349 systems.[1] Of the 1349 systems, 923 systems were GMC (68%) and 426 were SMC (32%), (Figure 4-1).

The data from the inventory is not particularly well suited for a study of this kind; since it tends to obscure relations rather than clarify them. Thus, we find data on CPU's leased and owned with no corresponding data on systems. In another area we find aggregate data on the value of GMC systems by purchase price category without regard for whether the systems are leased or owned.

Recognizing the deficiencies of using the data in the Inventory, special runs were requested from GSA to obtain data believed needed for this study. While the runs produced more useful breakdowns they did not adequately distinguish between leased and owned systems or provide data on the average annual cost of systems or CPU's taking into account the different payout rates one might assume depending on whether the system is leased or owned.

To overcome these difficulties and to produce the data needed for later parts of the study, the data available was used to provide estimates of a systems and CPU's costs on a yearly basis. It is further noted that the conclusions and results of this study are not highly sensitive to the precise values used in these estimates.

Since the inventory data is for both GMC and SMC systems, and our interest is primarily in GMC systems, it has been assumed that the distribution of the number of systems in each category (SMC, GMC) is in proportion to the totals 923/1349[2], (68%) GMC systems and 426/1349, (31%) SMC systems. In the case of CPU's, we

[1] All data from (INV 74) unless otherwise noted

[2] See Table 1 (INV 74), Summary

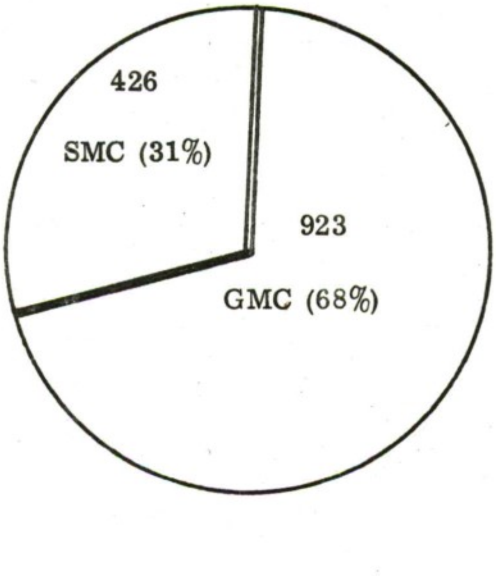


Figure 4-1. Distribution of USAF Computer Holdings, 1974

assumed the distribution is proportional to the totals 1022/1577 (64%) GMC CPU's and 555/1577 (35%) SMC CPU's.

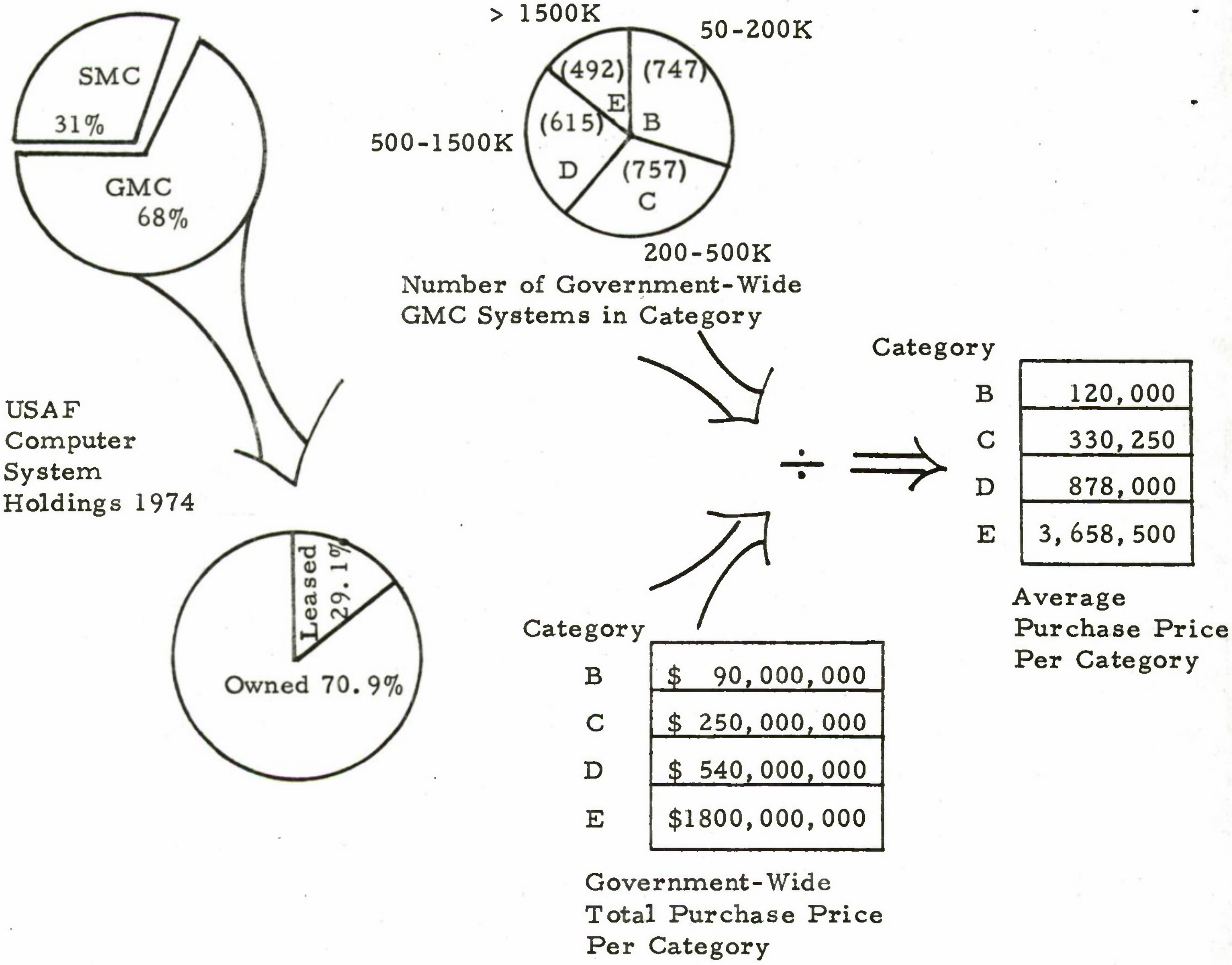
We have data giving the total number of both GMC and SMC systems in each of several purchase price categories. Since, SMC systems are not considered in this analysis, it is necessary to separate as much as possible the SMC data from the totals. If we assume that the proportion of GMC and SMC systems is the same for each price category, then multiplying each entry by the rate for GMC systems will give the desired numbers.

Total Number of GMC + SMC Systems	(x68.4%)	Number of GMC Systems	Purchase Price Category ($)
218		149	0 - 50K
329		225	50 - 200K
408		279	200K - 500K
213		146	500K - 1.5M
181		124	1.5M
1349		923	

Table 4-1. Derivation of Number of GMC Systems by Purchase Price Category

The purchase price category of systems corresponds to those shown in Chart 8 of the Inventory. We are interested in the average purchase price per category which we will take simply as the total dollar value shown divided by the total number of systems in the category. Small systems (less than $50,000 purchase price) were not considered, since these are expected to be used primarily in single classification level environments; as a result some systems affected by security considerations will not be included in this analysis.

The average purchase price of each category (based on Government-wide totals (omitting the small system category) is shown below. Its derivation is shown in Figure 4-2.



Category	
B	$ 90,000,000
C	$ 250,000,000
D	$ 540,000,000
E	$1800,000,000

Government-Wide Total Purchase Price Per Category

Category	
B	120,000
C	330,250
D	878,000
E	3,658,500

Average Purchase Price Per Category

Figure 4-2. Average Purchase Price of GMC Systems

Category	Government-Wide Number of GMC Systems in Category	Purchase Price Totals for Category	Average Purchase Price
B $50,000 to $200,000	747	$90,000,000	$120,480
C $200,000 to $500,000	757	$250,000,000	$330,250
D $500,000 to $1,500,000	615	$540,000,000	$878,000
E over 1.5 million	492	$1,800,000,000	$3,658,500

Table 4-2. Average Purchase Price of GMC Systems Based on Government-Wide Data (Table 8 (INV 74))

At the risk of appearing to be more accurate than the data allows, the average annual cost is normalized to a pseudo-rental cost using the relationships

$$\frac{\text{'purchase price'}}{4} = \text{annual rental for } \underline{\text{leased}} \text{ systems}$$

$$\frac{\text{'purchase price'}}{7} = \text{annual 'rental' for } \underline{\text{owned}} \text{ systems}$$

The latter relationship recognizes the useful life of a system is on the order of 6-8 years. Since there is no data on the number of leased and owned systems, we will assume them to be in proportion to the number of leased and owned CPU's (given in the summary of Systems and CPU's by Agency and Department (INV 74) p. 196) 725/1022 (70.9%) of the GMC CPU's are owned. Applying this rate to the base of 923 GMC systems, gives 655 systems owned, and 268 systems leased.

If the number of leased and owned systems in each price category is assumed to be proportional to the number of leased and owned CPU's in each category, the distribution for leased and owned GMC systems shown in the following table can be developed. The various data elements are summarized in Table 4-3; the derivation of the elements is indicated in Figure 4-4.

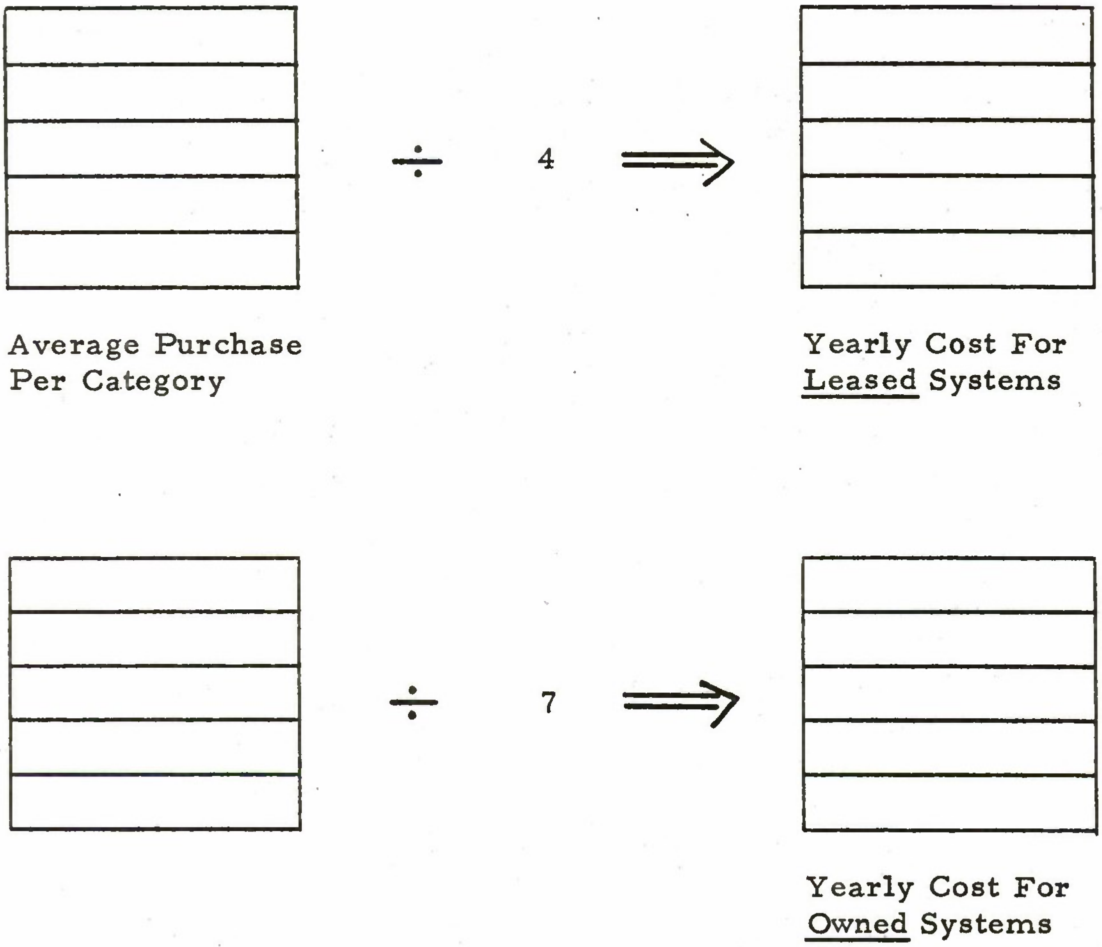

÷ 4 ⟹
Average Purchase Per Category
Yearly Cost For Leased Systems
÷ 7 ⟹
Yearly Cost For Owned Systems

Figure 4-3. Derivation of Yearly Costs

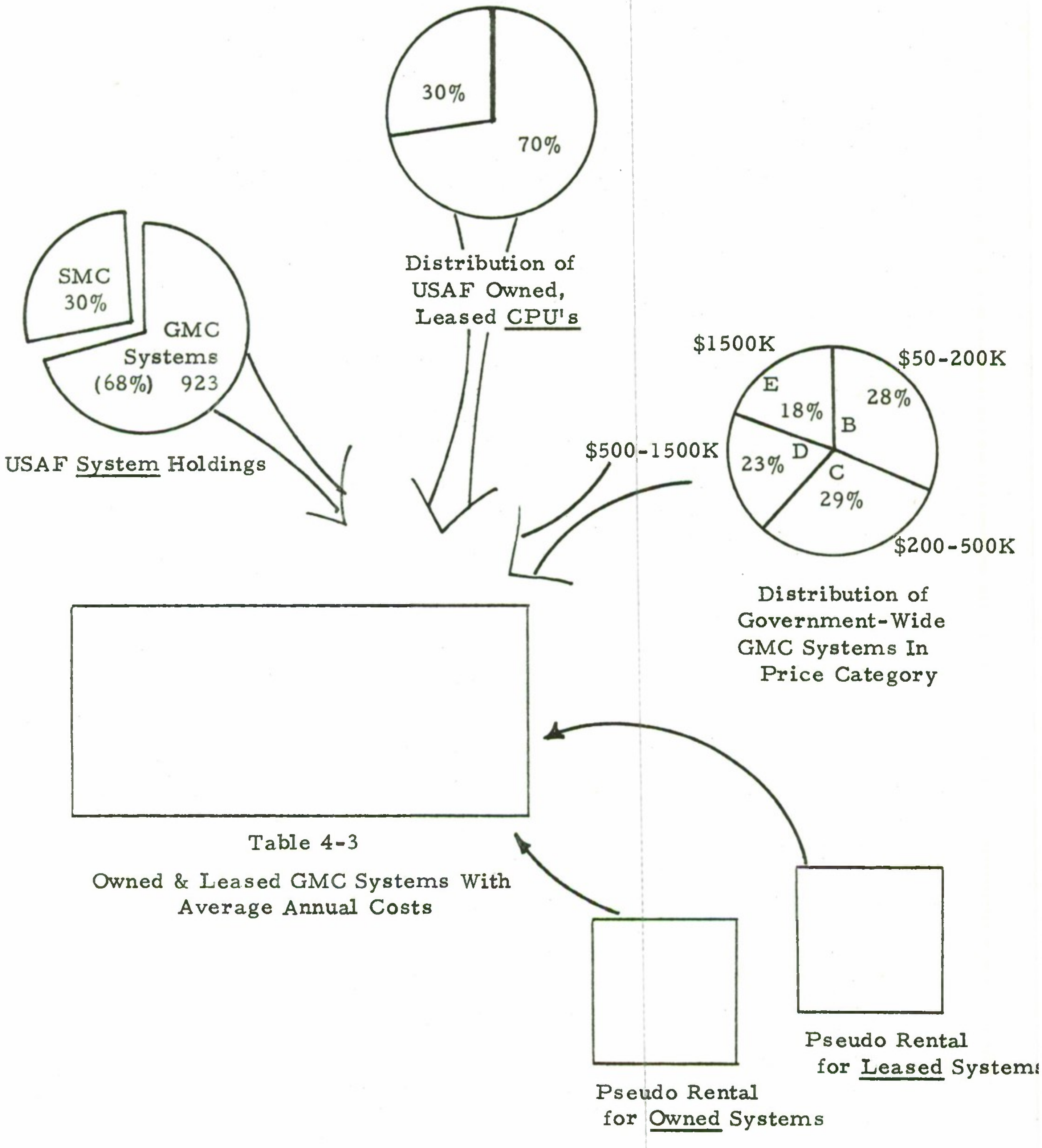


Figure 4-4. Derivation of Data Components of Cost Study

Table 4-3. Owned and Leased GMC Systems With Average Annual Costs

Purchase Price Category	Total GMC Systems	GMC Sys. Owned (70.9%)	GMC Sys. Leased (29.1%)	Average Yearly Cost Owned	Average Yearly Cost Leased
B	225	159	66	$ 17,200	$ 30,120
C	279	198	81	$ 47,200	$ 82,500
D	146	104	42	$125,400	$219,500
E	124	88	36	$522,600	$914,600
Total	774	549	225		

4.3 COST OF "AVOIDING" SECURITY PROBLEMS

Since there is not currently a 'solution' to the multi-level security problem, the Air Force (and other organizations) use one or more of the avoidance techniques discussed earlier. For this study, the percentage and number of installations using a specific technique predominantly was estimated. These estimates are shown in Figure 4-5.

There is no special justification for the figures used. Except that they are in rough balance with what has been observed by the author. Since the author's (or anyone else's) experience is limited, any other 'mix' may be substituted.

The security problem avoidance techniques have been discussed previously except for the category 'no problem' which is meant to cover systems and places where no classified processing is done at all.

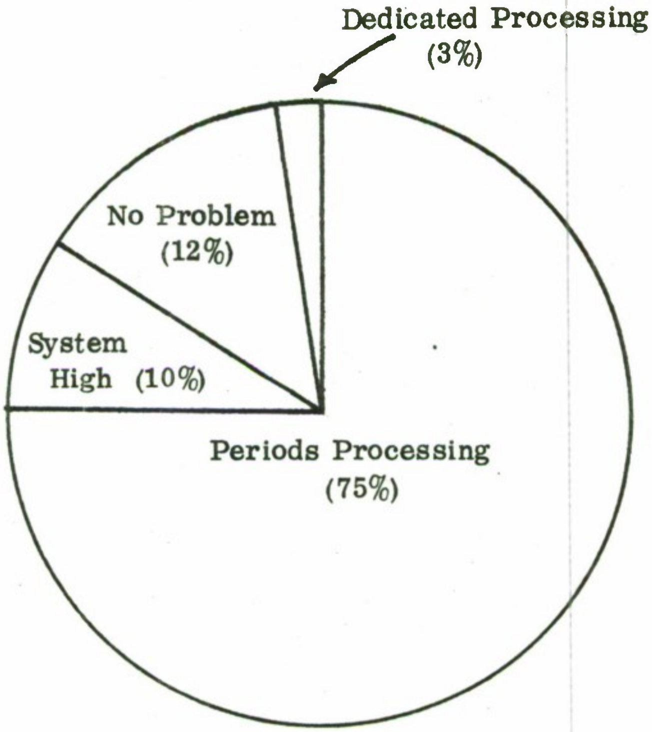


Figure 4-5. Estimated Distribution of Security Avoidance Techniques

Figure 4-5 is the figure to change in applying the cost evaluation methodology if any other 'mix' of avoidance technique is preferred.

4.3.1 Dedicated Processors

As discussed in Section 3.2, the data of interest is the cost of the estimated 25% overage overcapacity due to use of dedicated processing to avoid security problems. We can obtain this directly, using the data in Table 4-4.

Taking 3% of the total to represent the portion of systems using the dedicated processors technique and 25% of that total to represent the costs due to security gives the annual cost of a little under one million dollars.

4.3.2 Periods Processing

The periods processing (SCH 75) cost is almost entirely due to the lost capacity at changeover. The cost is treated here as an increase in the utilization cost of the system. The amount of time it takes to effect a change of processing classification depends primarily on the size of the system.

Data was obtained from GSA that gives the number of systems (both SMC and GMC) in each purchase price category by the hours of utilization. To utilize this data, it was assumed that smaller systems (Purchase Price Categories B, C) can be changed over in 10 minutes, and larger systems (Purchase Price Categories D and E) can be changed in 20 minutes. Further, it is assumed that there are two transitions per day (one from unclassified to classified, one from classified to unclassified).

In determining costs for periods processing, it was decided to base the costs on utilization rather than total available time.

Table 4-4. Costs For Dedicated Processing

	A	B	C	D	E	F	G
Purchase Price Category	GMC Systems Owned	Avg. Yearly Cost (Owned)	(A x B)	GMC Systems Leased	Avg. Yearly Cost (Leased)	(D x E)	(C + F)
B	159	$ 17,200	2,734,800	65	$ 30,120	1,957,800	4,692,600
C	198	$ 47,200	9,345,600	81	$ 82,500	6,682,500	16,028,100
D	104	$125,400	13,041,600	42	$219,500	9,219,000	22,260,600
E	88	$522,600	45,988,800	36	$914,600	32,925,600	78,914,400
			71,110,800			50,784,900	121,895,700
					(Estimated % of USAF systems using the technique)		x .03
							$ 3,656,871
					(Estimated Average Overcapacity)		x .25
				Annual 'Cost' of Dedicated Processing			$ 914,217

While it could be argued that if a system is not fully utilized, there is no "cost" associated with a color change, this would not be the case if the system were fully utilized.

Whether or not a system is fully utilized is not the issue. The military departments often purchases excess capacity in systems in order to handle 'surge' processing requirements or in anticipation of applications growth.

Table 4-5. Hours of Utilization by Purchase Price Category

		Number of Systems (SMC + GMC Reporting - Purchase Price Category			
% Utilization	Hrs. of SVC*	B	C	D	E
		126 = 0	81 = 0	59 = 0	58 = 0
0 - 10	37	20	3	0	0
10 - 20	111	17	5	4	0
20 - 30	184	43	21	7	5
30 - 40	257	11	16	6	3
40 - 50	330	13	29	19	9
50 - 60	403	7	39	41	5
60 - 70	476	12	49	28	16
70 - 80	549	6	55	11	16
80 - 90	622	18	42	11	30
90 - 100	695	56	68	27	39
	TOTALS	329	408	213	181

* The midpoint of the range is used for hours of service. Using the midpoint introduces approximately - 1% error in the number of hours. A maximum of 730 hours (per month) is reported in the data.

The data on system utilization gave a count of the number of systems (both SMC and GMC) reporting a utilization of N hours. Thus, for example, in the purchase price category of greater than 1.5 million, there were two systems reporting hours in service of 530 (per month), 1 reporting 542 hours, 1 reporting 547 hours, etc.

This data was grouped by purchase price category into the number of systems reporting 0 - 10% (0 - 73 hrs) utilization; 10 - 20% (74 - 146 hrs) ... etc. Table 4-6 shows the groupings.

If the effective utilization of a system is reduced because of color change time, then either the effective planned capacity is reduced or the effect of color changing was built into the initial system sizing. In either case, there is a cost associated with the security avoidance technique.

We define a cost of 'ownership' as cost/hrs. owned. The 'costs' are those from Table 4-3 (owned and leased GMC Systems with Average Annual Costs). Ownership costs by purchase price categories are shown for leased and owned systems in Figure 4-7. The differences are in the payout period assumed. See Section 4-2 for a discussion of this point.

Table 4-6

Hourly 'Ownership' Costs by Purchase Price Category
(Yearly Costs/8760 = Hourly Rate)

Purchase Price Category	Owned Systems	Leased Systems
B	$ 1.96	$ 3.44
C	$ 5.38	$ 9.42
D	$14.31	$ 25.05
E	$59.65	$104.40

The computation of the cost of periods processing requires evaluation of the following expression.

		Annual		Number of		
Average Hrs. Utilized	x	Cost of System	x	Systems	x	Reduction of
		(owned, leased)		(owned, leased)		Effective Utilization

Since the data is already grouped by average hours utilized, the number of systems reported for each overage utilization were distributed between owned and leased systems by taking 70.9% as owned (to the nearest whole number) and the difference as leased.

The reduction of effective utilization is taken from Table 4-7 where it is computed independently.

Percent Utilization (Midpoint of Range)	Reduction of effective utilization when changeover time t equals	
	10 minutes	20 minutes
5	.281	.562
15	.091	.182
25	.054	.109
35	.04	.08
45	.03	.03
55	.024	.049
65	.02	.04
75	.018	.036
85	.016	.032
95	.014	.028

Table 4-7

Reduction of Effective Utilization

$(1 - \frac{U - NT}{U})$ as a function of percent of utilization

Table 4-8(a)

Monthly Costs of Periods Processing

Purchase Price Category B ($50, 000 - $200, 000)

A		B		C		G	D		E		H	F
Average Hrs. Utilized	x	Cost Rate (Owned)	x	Number of Systems	x	(AxBxCxF)	Cost Rate (Leased)	x	Number of Systems	x	(AxDxExF)	Utilization Reduction Factor
37		$1. 96		14		285	$3. 44		6		215	. 281
111		1. 96		12		237	3. 44		5		174	. 091
184		1. 96		30		540	3. 44		13		411	. 05
257		1. 96		8		161	3. 44		3		106	. 04
330		1. 96		9		175	3. 44		4		106	. 03
403		1. 96		5		95	3. 44		2		67	. 024
476		1. 96		8		149	3. 44		4		131	. 02
549		1. 96		4		77	3. 44		2		68	. 018
622		1. 96		13		254	3. 44		5		171	. 016
695		1. 96		39		744	3. 44		17		569	. 014
						2717/mo.					2018/mo.	

$ 2, 717
$ 2, 018

$ 4, 735/mo.
x 12

$56, 820/yr.

Table 4-8 (b)

Monthly Costs of Periods Processing

Purchase Price Category C ($200,000 - $500,000)

A		B		C		G	D		E		H	F
Average Hrs. Utilized	x	Cost Rate (Owned)	x	Number of Systems	x	(AxBxCxF)	Cost Rate (Leased)	x	Number of Systems	x	(AxDxExF)	Utiliza Reduct Facto
37		5.38/hr.		2		111	9.42/hr.		1		97	.27
111		5.38/hr.		4		217	9.42/hr.		1		95	.92
184		5.38/hr.		15		242	9.42/hr.		6		520	.05
257		5.38/hr.		11		608	9.42/hr.		5		484	.04
330		5.38/hr.		20		1065	9.42/hr.		9		839	.03
403		5.38/hr.		27		1405	9.42/hr.		12		1093	.024
476		5.38/hr.		34		1741	9.42/hr.		15		1345	.020
549		5.38/hr.		39		2073	9.42/hr.		16		1489	.018
622		5.38/hr.		29		1553	9.42/hr.		13		1219	.016
695		5.38/hr.		48		2513	9.42/hr.		20		1833	.014
						12028					9014	

$12,028
$ 9,014

$21,042/mo.
x 12

$252,504/yr.

Table 4-8(c)

Monthly Costs of Periods Processing

Purchase Price Category D ($500,000 - $1.5 million)

A		B		C		G	D		E		H	F
Average Hrs. Utilized	x	Cost Rate (Owned)	x	Number of Systems	x	(AxBxCxF)	Cost Rate (Leased)	x	Number of Systems	x	(AxDxExF)	Utilization Reduction Factor
37		$14.31		0			$25.05		0			.54
111		$14.31		3		857	$25.05		1		500	.18
184		$14.31		5		1316	$25.05		2		921	.10
257		$14.31		4		1176	$25.05		2		1030	.08
330		$14.31		13		3683	$25.05		6		2975	.06
403		$14.31		29		8027	$25.05		12		5815	.048
476		$14.31		20		5449	$25.05		8		3815	.04
549		$14.31		8		2262	$25.05		3		1485	.036
622		$14.31		8		2278	$25.05		3		1496	.032
695		$14.31		19		5291	$25.05		8		3900	.028
						30339					21937	

$ 30,339
$ 21,937

$ 52,276/mo.
x 12

$627,312/yr.

Table 4-8(d)

Monthly Costs of Periods Processing
Purchase Price Category E (> 1.5 million)

A Average Hrs. Utilized	x	B Cost Rate (Owned)	x	C Number of Systems	x	G (AxBxCxF)	D Cost Rate (Leased)	x	E Number of Systems	x	H (AxDxExF)	F Utilizatio Reductio Factor
37		$59.62		0			$104.40					.54
111		$59.62		0			$104.40					.18
184		$59.62		4		4388	$104.40		1		1920	.10
257		$59.62		2		2451	$104.40		1		2146	.08
330		$59.62		6		7082	$104.40		3		6201	.06
403		$59.62		4		4613	$104.40		1		2019	.048
476		$59.62		11		12486	$104.40		5		9938	.04
549		$59.62		11		12961	$104.40		5		10316	.036
622		$59.62		21		24920	$104.40		9		18701	.032
695		$59.62		28		32485	$104.40		1		22347	.028
						101386					73588	

```
 $101,386
 $ 73,588
 ________
 $174,974/mo.
     x  12
 ________
$2,099,688/yr.
```

The detailed data of Table 4-8(a) through 4-8(d) gives only gross monthly costs assuming all USAF systems were using only periods processing. Summing the monthly costs of each purchase price category and multiplying by 12 gives the gross yearly costs. Taking 75% (the estimate of the number of USAF systems using the technique) of that gives an annual cost of periods processing of approximately $2,253,000.

4.3.3 System High

Typical systems, regardless of their physical size have between 30 and 50 'users'. Users in this case are offices or other organizational entities who use computers for management, planning, and control. Specifically excluded are professional programmers, system analysts and similar personnel operating to support users of the kind noted above.*

Each 'user' as defined above may have from 2 to possibly 10 individuals who are authorized to submit work to and accept results from a computer system.

While occassionally it will occur that programming and other support staff do not have appropriate clearances for system high operation, more frequently an entire office, or a significant number of those authorized to 'use' a system do not have the needed clearances.

The average cost of obtaining a higher clearance is difficult to establish. Independent inquiry into this matter elicited a figure of $281 for the cost of a background investigation alone. A clearance is variously estimated at $350 and up. Some sources indicate well over $5,000 for any of the special clearances. For this estimate we will use $1,000 for new clearances SECRET or above.

The number of 'new' clearances required each year at an installation is a function of the turnover rate and the proportion of uncleared (for the system high level) personnel to the total new personnel. The cost of 'new' clearances each year is then given by:

* Excluding programming and other computer support personnel from this estimate results in lower costs being allocated to this avoidance technique than would otherwise be expected.

$$\begin{array}{c}\text{turnover}\\\text{rate}\end{array} \times \begin{array}{c}\text{proportion of}\\\text{uncleared to}\\\text{total number}\\\text{of new users}\end{array} \times \begin{array}{c}\text{number of}\\\text{users per}\\\text{installation}\end{array} \times \begin{array}{c}\text{number of}\\\text{installations}\end{array} \times \begin{array}{c}\text{cost}\\\text{per}\\\text{clearance}\end{array} \times \begin{array}{c}\text{proportion of}\\\text{total systems}\\\text{using system}\\\text{'high' as an}\\\text{avoidance technique}\end{array} .$$

A turnover rate of 15% and a proportion of uncleared to total new users of 1 in 8 or 12.5% is used.

In the Inventory, there are 113 CONUS locations named as the sites of various kinds of systems and 150 located "overseas." While a few of these installations are undoubtedly unique SMC systems, we have lumped them all together and are dealing with approximately 263 USAF system installations. (There is even greater error due to treating such locations as 'Washington, DC" or SCOTT AFB as a single installation when they are known to be the site of multiple installations.)

An average of 300 'users' (as described above) per installation is used.

With these data, the annual cost of system high operations is:

.15 x .125 x 300 x 263 x $1000 x .1 = $148,000

4.3.4 Summary of Current Security Costs*

The annual costs of security problem avoidance is shown in the table below:

Technique	Cost
Dedicated Processing	$900,000
Periods Processing	$2,250,000
System High	$148,000
	$3,357,000

Table 4-9. Summary of Estimated Current Costs of Avoidance Techniques

* It should be clearly understood that these estimates involve only current readily identified continuing costs. If the analysis had attempted to take into account additional costs due to lack of solutions to the problem, (e.g. requirement to secure all communications lines connected to a computer system containing classified data regardless of the classification of work actually handled by the links; requirement to physically protect terminals at the level of the classification of data contained in the systems, etc.) the costs would be many times higher.

4.4 FUTURE SYSTEMS COSTS

Future systems security costs are both the cost of obtaining secure systems and the increased costs of operations if such systems are not available.

Basically, the increased operations cost factors are those previously discussed as costs of security problem avoidance plus an undeterminable cost of not making effective use of systems because of security problems. It is most unlikely that the objectives planned for new(er) systems of more on-line, interactive working and more accurate, timely, and meaningful reporting for management purposes and the like will be surrendered. The consequence is that more of the avoidance techniques that completely eliminate security problems (i.e. systems high and dedicated processors) will be used. The number and percentage of installations using these techniques can be expected to increase if proper internal controls are not put into newer systems for which hardware will be acquired in the 1975-1980 time frame.

What of the future? Using data from the Inventory, the Federal Government as a whole has increased its use of computers by the following amounts over the 5 and 4 year periods shown.

Type of System	Average Annual Increase % (1970-1974)	Average Annual Increase (1971 - 74)
SMC	21½%	23%
GMC	2.8%	0.5%
Combined	10.3%	10%

Table 4-10. Government Wide Growth in Use of Computers

The lack of growth in the GMC category is suspicious on the surface, however, the rapid growth rate for SMC systems suggests that there is an incentive for reporting new systems in the SMC category. Alternatively one would be led to believe that the entire government was acquiring only new Special Management Category systems, while retaining or replacing GMC systems on a one-for-one basis. This is not likely.

A similar phenomenon is evident in data for the USAF which shows the following pattern.

Type of System	1970	1971	1972	1973	1974
SMC	169	232	315	387	426
GMC	993	975	1000	962	923
TOTAL	1162	1207	1315	1349	1349

Growth Rate of USAF GMC System - - 1.8%

Growth Rate of Total USAF Systems - 3.8%

Table 4-11

The combined figure of 3.8% is used since it is believed to accurately reflect the true growth of computer use in the Air Force.

The 3.8%/year growth in computer holdings is projected forward for 6 and 11 years giving estimates of the number of systems held by the USAF in 1980 and 1985. Thus, in 1980 one expects on the order of 1655 USAF systems, and in 1985 approximately 1912 systems.

4.5 SOLUTION METHODS

In analyzing the impact of a particular solution method, we recognize that the solution methods are not universally applicable and wish to take this into account. As an example, the Job Stream Separator (JSS) can only be effectively used in those installations where classified processing can be anticipated and "scheduled" in some sense. It is not a suitable solution method for those installations having a continuous (albeit not totally system-consuming) classified workload or where the classified application(s) must be on-line to satisfy availability requirements. Likewise, secure VM systems are a solution primarily to hardware sharing requirements. While it is technically possible to consider a limited form of data sharing in the VM context, such sharing would be grossly inefficient and is better handled in the certified systems approach.

It should also be evident that given a certified data sharing system, the need to consider VM's is eliminated, since the data sharing systems must include as an integral part of their design the demonstrated ability to isolate users one from another — thus, subsuming VM systems.

While a variety of cost comparisons could be developed, we are interested in what cost impact could be expected from pursuing each of the "solution" techniques exclusively, recognizing the application limitations associated with JSS and VM's.

JSS seen as a solution alternative to periods processing (as a higher speed method) is straight forward. Less obvious is how to allocate VM's. In examing the cases, it was decided that VM's could be considered a solution alternative for dedicated processors because dedicated processors have no special implication of data sharing, while 'system high' operation has an implication that some data is shared. The association of VM with dedicated processors was made accordingly.

Finally, the costs associated with Certified Systems are computed assuming that the Certified Systems are applied to a base that includes the systems in both the dedicated processing and systems high categories.

All of these various approaches are compared with the expected costs of using the avoidance techniques described above.

4.5.1 Costs of Avoidance Techniques 1980, 1985

Simple extrapolation of the current estimated avoidance costs result in the following:

Cumulative Costs

1974 - 1980	1974 - 1985
$19,985,000 - $21,170,000*	$36,630,000 - $44,460,000*

*Simple and compound growth at 3.8%

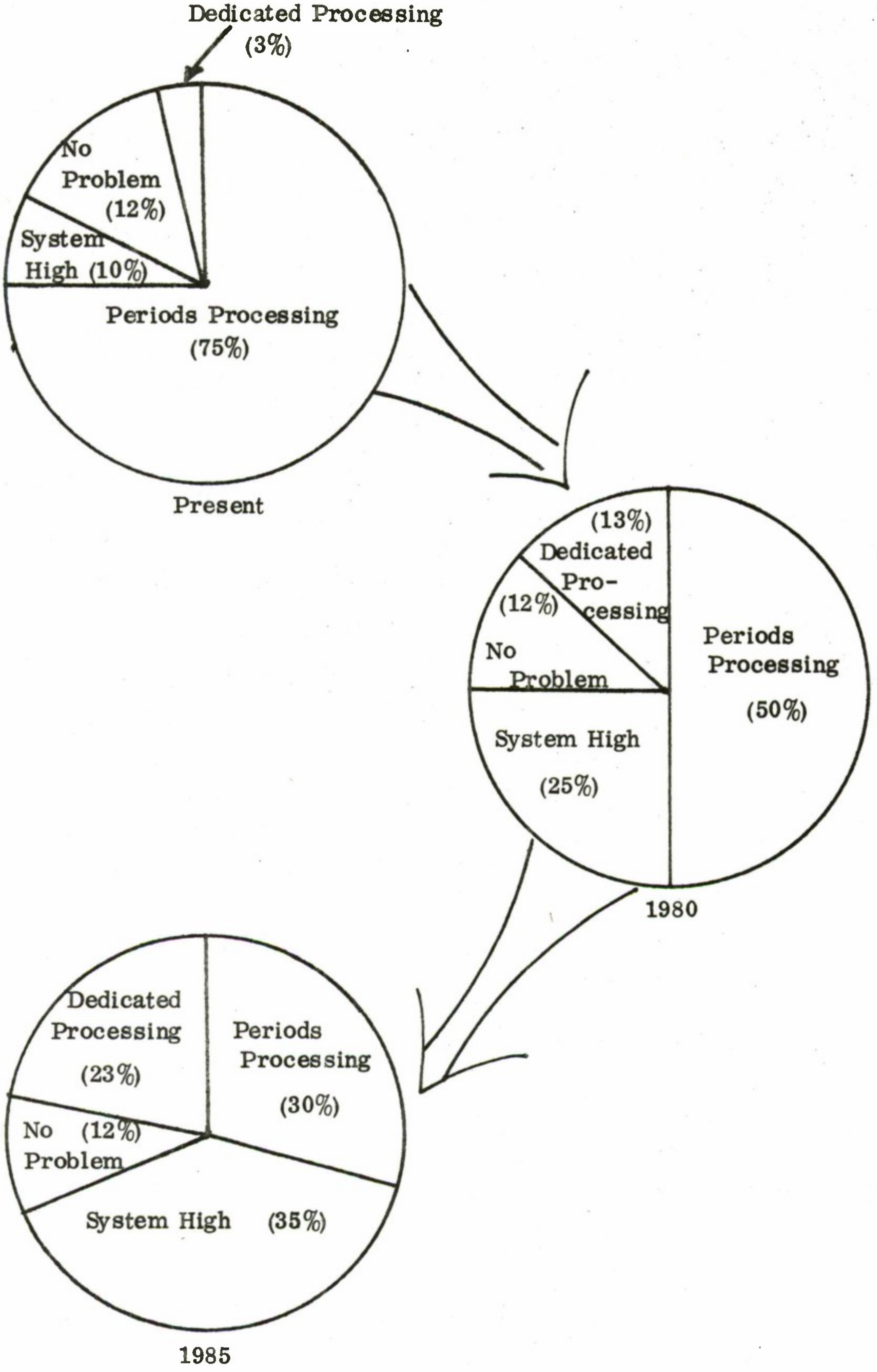


Figure 4-6. Change in Estimated Distribution of Security Problem Avoidance Techniques

Average Annual Costs

1980 (Base 1655 Systems)	1985 (Base 1912 Systems)
$3,940,000/yr	$4,550,000/yr

However, such a simple extrapolation would not adequately take into account known trends that contribute more pressure for at least hardware sharing, as well as more requirements for data sharing.

The trends that are evident include; increased use of interactive/remote terminals, greater integration of computers into on-going operational daily routine (computer itself less visible to users), greatly increased use of networking for making computer available to users.

The results of these trends is to change the distribution of the security problem avoidance techniques used. Reflecting increased on-line and real-time working, it is expectedthat periods processing can be used less frequently as a security problem avoidance technique, and that there will be an increase in the percentage of installations using dedicated processors and/or system high operation. Accordingly, the distribution in table 4-12 was changed to reflect these trends. This is shown in the table below:

Technique	Est. % of USAF Installations using in 1980	Change from Figure 4-5	Est. % of USAF Installations using in 1985	Change from Figure 4-5
Dedicated Processors	13	+10	23	+20
Periods Processing	50	-25	30	-45
System High	25	+15	35	+25
No Problem	12	0	12	0

Table 4-12

Estimated Distribution of Security Problem Avoidance Techniques for 1980, 1985

Using the modified distribution of security problem avoidance techniques shown in Table 4-12 and the projected number of systems of 1655 (1980) and 1912 (1985) the costs for dedicated processors is shown in the following two tables.

	A	B	C	D	E	F	G
Purchase Price Category	GMC Systems (owned)	Average Yearly Cost (owned)	(A x B)	GMC Systems (leased)	Average Yearly Cost (leased)	(D x E)	(C + F)
B	195	$ 17,200	$ 3,354,000	81	$ 30,120	$ 2,440,000	$ 5,794,000
C	243	$ 47,200	$11,470,000	99	$ 82,500	$ 8,168,000	$ 19,638,000
D	128	$125,400	$16,051,000	52	$219,500	$11,414,000	$ 27,465,000
E	108	$522,600	$56,440,000	44	$914,600	$40,242,000	$ 96,682,000
	674		$87,315,000	276		$62,264,000	$149,579,000

	$149,579,000
	x.13
	$ 19,445,000
	x.25
Average Annual Cost of Dedicated Processing	$ 4,861,000

Table 4-13(a). Average Annual Cost of Dedicated Processing 1980

	A	B	C	D	E	F	G
Purchase Price Category	GMC Systems (owned)	Average Yearly Cost (owned)	(A x B)	GMC Systems (leased)	Average Yearly Cost (leased)	(D x E)	(C + F)
B	225	$ 17,200	$ 3,870,000	94	$ 30,120	$ 2,831,000	$ 6,701,000
C	281	$ 47,200	$ 13,263,000	115	$ 82,500	$ 9,488,000	$ 22,751,000
D	147	$125,400	$ 18,434,000	59	$219,500	$12,951,000	$ 31,385,000
E	125	$522,600	$ 65,325,000	51	$914,600	$46,645,000	$111,970,000
	778		$100,892,000	319		$71,915,000	$172,807,000
					$172,807,000		
					x .23		
					$ 39,745,000		
					x .25		
Average Annual Cost of Dedicated Processing					$ 9,930,000		

Table 4-13(b). Average Annual Costs of Dedicated Processing, 1985

The following 8 tables develop the costs of periods processing expected in 1980 and 1985. The costs are the sum of the annual costs for each purchase price category multiplied by the percent of USAF systems expected to be utilizing periods processing in 1980 and 1985. This is summarized below.

Purchase Price Category	Total Annual Costs For Periods Processing (All Systems)	
	1980	1985
B	$ 143,736	$ 160,960
C	$ 622,092	$ 712,200
D	$ 773,256	$ 811,080
E	$2,584,980	$2,995,000
	$4,124,064	$4,679,240
	x .50	x .30
	$2,062,000	$1,403,000

Table 4-14. Summary of Annual Costs of Periods Processing, 1980-1985

A		B		C		G	D		E		H	F
Average Hrs. Utilized	x	Cost Rate (Owned)	x	Number of Systems	x	(AxBxCxF)	Cost Rate (Leased)	x	Number of Systems	x	(AxDxExF)	Utilization Reduction Factor
37		$1.96		17		$ 666	$3.44		8		$ 550	.54
111		$1.96		15		$ 587	$3.44		6		$ 412	.18
184		$1.96		37		$1,334	$3.44		16		$1,012	.10
257		$1.96		9		$ 362	$3.44		5		$ 354	.08
330		$1.96		11		$ 427	$3.44		5		$ 340	.06
403		$1.96		6		$ 227	$3.44		3		$ 200	.048
476		$1.96		10		$ 551	$3.44		5		$ 327	.04
549		$1.96		5		$ 193	$3.44		2		$ 136	.036
622		$1.96		15		$ 585	$3.44		7		$ 479	.032
695		$1.96		48		$1,830	$3.44		21		$1,406	.028
						$6,762					$5,216	

$5,216
$6,762

$11,978/mo.

x 12

$143,736/yr.

Table 4-14(a). Periods Processing Costs, Purchase Price Category B, 1980

A		B		C		G	D		E		H	F
Average Hrs. Utilized	x	Cost Rate (Owned)	x	Number of Systems	x	(AxBxCxF)	Cost Rate (Leased)	x	Number of Systems	x	(AxDxExF)	Utilizati Reductic Factor
37		$5.38		3		$ 322	$9.42		1		$ 188	.54
111		$5.38		4		$ 430	$9.42		2		$ 376	.18
184		$5.38		18		$ 1,781	$9.42		8		$ 1,387	.10
257		$5.38		14		$ 1,549	$9.42		6		$ 1,162	.08
330		$5.38		25		$ 2,663	$9.42		11		$ 2,052	.06
403		$5.38		33		$ 3,434	$9.42		14		$ 2,551	.048
476		$5.38		42		$ 4,302	$9.42		18		$ 3,228	.04
549		$5.38		46		$ 4,891	$9.42		21		$ 3,910	.036
622		$5.38		36		$ 3,855	$9.42		16		$ 3,000	.032
695		$5.38		59		$ 6,177	$9.42		25		$ 4,583	.028
						$29,404					$22,437	

$22,437
$29,404

$ 51,841/mo.

x 12

$622,092/yr.

Table 4-14 (b). Periods Processing Costs, Purchase Price Category C, 1980

A Average Hrs. Utilized	x	B Cost Rate (Owned)	x	C Number of Systems	x	G (AxBxCxF)	D Cost Rate (Leased)	x	E Number of Systems	x	H (AxDxExF)	F Utilization Reduction Factor
37		$14.31		0		0	$25.05		0		0	.54
111		$14.31		3		$ 857	$25.05		2		$ 1,001	.18
184		$14.31		6		$ 1,580	$25.05		2		$ 922	.10
257		$14.31		5		$ 1,471	$25.05		2		$ 1,030	.08
330		$14.31		16		$ 4,533	$25.05		7		$ 3,472	.06
403		$14.31		35		$ 9,688	$25.05		15		$ 7,268	.048
476		$14.31		24		$ 6,539	$25.05		11		$ 4,722	.04
549		$14.31		9		$ 2,545	$25.05		5		$ 2,475	.036
622		$14.31		9		$ 2,563	$25.05		5		$ 2,492	.032
695		$14.31		23		$ 6,405	$25.05		10		$ 4,875	.028
				130		$36,181			59		$28,257	

$ 28,257

$ 36,181

$ 64,438/mo.

x 12

$773,256/yr.

Table 4-14(c). Periods Processing Costs, Purchase Price Category D, 1980

Purchase Price Category E (> 1. 5 million)

A		B		C		G	D		E		H	F
Average Hrs. Utilized	x	Cost Rate (Owned)	x	Number of Systems	x	(AxBxCxF)	Cost Rate (Leased)	x	Number of Systems	x	(AxDxExF)	Utilizatio Reductio Factor
37		$59.62		0		0	$104. 40		0			. 54
111		$59.62		0		0	$104. 40		0			. 18
184		$59.62		4		$ 4,388	$104. 40		2		$ 3,842	. 10
257		$59.62		2		$ 2,451	$104. 40		1		$ 2,146	. 08
330		$59.62		8		$ 9,443	$104. 40		3		$ 6,201	. 06
403		$59.62		4		$ 4,613	$104. 40		2		$ 4,039	. 048
476		$59.62		14		$ 15,892	$104. 40		6		$11,926	. 04
549		$59.62		14		$ 16,496	$104. 40		6		$12,380	. 036
622		$59.62		26		$ 30,853	$104. 40		11		$22,857	. 032
695		$59.62		34		$ 39,446	$104. 40		14		$28,442	. 028
						$123,582					$91,833	

$ 91,833
$ 123,582

$ 215,415/mo.
x 12

$2,584,980/yr.

Table 4-14(d). Periods Processing Costs, Purchase Price Category E, 1980

Purchase Price Category B ($50,000 - $200,000)

A		B		C		G	D		E		H	F
Average Hrs. Utilized	x	Cost Rate (Owned)	x	Number of Systems	x	(AxBxCxF)	Cost Rate (Leased)	x	Number of Systems	x	(AxDxExF)	Utilization Reduction Factor
37		$1.96		20		$ 783	$3.44		8		$ 550	.54
111		$1.96		17		$ 666	$3.44		7		$ 481	.18
184		$1.96		43		$1,551	$3.44		18		$1,139	.10
257		$1.96		11		$ 443	$3.44		5		$ 354	.08
330		$1.96		13		$ 505	$3.44		5		$ 340	.06
403		$1.96		7		$ 265	$3.44		3		$ 200	.048
476		$1.96		12		$ 448	$3.44		5		$ 327	.04
549		$1.96		6		$ 232	$3.44		3		$ 204	.036
622		$1.96		18		$ 702	$3.44		8		$ 548	.032
695		$1.96		56		$2,136	$3.44		23		$1,540	.028
						$7,731					$5,683	

$5,683
$7,731

$13,414/mo.
x 12

$160,960/yr.

Table 4-14(e). Periods Processing Costs, Purchase Price Category B, 1985

Purchase Price Category C ($200,000 - $500,000)

A		B		C		G	D		E		H	F
Average Hrs. Utilized	x	Cost Rate (Owned)	x	Number of Systems	x	(AxBxCxF)	Cost Rate (Leased)	x	Number of Systems	x	(AxDxExF)	Utilizatio Reductio Factor
37		$5.38		3		$ 322	$9.42		1		$ 188	.54
111		$5.38		5		$ 537	$9.42		2		$ 376	.18
184		$5.38		21		$ 2,079	$9.42		9		$ 1,560	.10
257		$5.38		16		$ 1,770	$9.42		7		$ 1,355	.08
330		$5.38		29		$ 3,089	$9.42		12		$ 2,238	.06
403		$5.38		39		$ 4,059	$9.42		16		$ 2,916	.048
476		$5.38		49		$ 5,019	$9.42		20		$ 3,587	.04
549		$5.38		55		$ 5,848	$9.42		23		$ 4,282	.036
622		$5.38		42		$ 4,498	$9.42		18		$ 3,375	.032
695		$5.38		68		$ 7,119	$9.42		28		$ 5,133	.028
						$34,340					$25,010	

$ 25,010
$ 34,340

$ 59,350/mo.
x 12

$712,200/yr.

Table 4-14(f). Periods Processing Costs, Purchase Price Category C, 1985

Purchase Price Category D ($500,000 - $1.5 million)

A		B		C		G	D		E		H	F
Average Hrs. Utilized	x	Cost Rate (Owned)	x	Number of Systems	x	(AxBxCxF)	Cost Rate (Leased)	x	Number of Systems	x	(AxDxExF)	Utilization Reduction Factor
37		$14.31					$25.05					.54
111		$14.31		4		$ 1,144	$25.05		2		$ 1,001	.18
184		$14.31		7		$ 1,843	$25.05		3		$ 1,383	.10
257		$14.31		6		$ 1,765	$25.05		3		$ 1,545	.08
330		$14.31		19		$ 5,383	$25.05		8		$ 3,968	.06
403		$14.31		14		$ 3,875	$25.05		17		$ 8,238	.048
476		$14.31		28		$ 7,629	$25.05		12		$ 5,723	.04
549		$14.31		11		$ 3,111	$25.05		5		$ 2,475	.036
622		$14.31		11		$ 3,133	$25.05		5		$ 2,493	.032
695		$14.31		27		$ 7,519	$25.05		11		$ 5,362	.028
						$35,402					$32,188	

$ 32,188
$ 35,402

$ 67,590/mo.
x 12

$811,080/yr.

Table 4-14(g). Periods Processing Costs, Purchase Price Category D, 1985

Purchase Price Category E (> 1. 5 million)

A		B		C		G	D		E		H	F
Average Hrs. Utilized	x	Cost Rate (Owned)	x	Number of Systems	x	(AxBxCxF)	Cost Rate (Leased)	x	Number of Systems	x	(AxDxExF)	Utilizatioı Reduction Factor
37		$59. 62		0			$104. 40		0			. 54
111		$59. 62		0			$104. 40		0			. 18
184		$59. 62		5		$ 5, 485	$104. 40		2		$ 3, 843	. 10
257		$59. 62		3		$ 3, 677	$104. 40		1		$ 2, 147	. 08
330		$59. 62		9		$ 10, 624	$104. 40		5		$ 10, 340	. 06
403		$59. 62		5		$ 5, 766	$104. 40		2		$ 4, 041	. 048
476		$59. 62		16		$ 18, 163	$104. 40		7		$ 13, 920	. 04
549		$59. 62		16		$ 18, 853	$104. 40		7		$ 14, 449	. 036
622		$59. 62		30		$ 35, 600	$104. 40		12		$ 24, 945	. 032
695		$59. 62		39		$ 45, 248	$104. 40		16		$ 32, 518	. 028
						$143, 416					$106, 203	

$106, 203
$143, 416

$249, 619/mo.
x 12

$2, 995, 000/yr.

Table 4-14 (h). Periods Processing Costs, Purchase Price Category E, 1985

Using the modified distribution of security problem avoidance techniques in Table 4-16, the cost range for avoidance techniques is:

	1980 (Base = 1655 systems) (in $ millions)	1985 (Base = 1912 systems) (in $ millions)
Dedicated Processors	$4,860,000	$ 9,930,000
Periods Processing	$2,062,000	$ 1,403,000
Systems High	$ 147,937	$ 207,112
	$7,070,000	$11,540,000

Table 4-15

Costs of Security Problem Avoidance Techniques 1980, 1985

The main component of the increases are due to the projected increased use of dedicated systems to avoid security problems.

4.5.2 Job Stream Separator

The Job Stream Separator automates the changeover functions associated with periods processing. The major cost elements are the development costs and the per-system special equipment costs. These costs are estimated at $685,000 and $75,000 respectively in (Sch 75). The time to effect a 'color change' with JSS is expected to be on the order of 10 minutes. The number of changes per day is expected to be 2. The average reduction in utilization (due to periods processing) over all purchase price categories and all utilizations is 3.2%.

The initial costs are;

$$I \times \$75{,}000 + \frac{\$685{,}000}{I} + .032\ C.$$

where I (= 828, half of the systems in 1980) is the number of systems and C is the cost of periods processing systems.

The $75,000 per system investment cost (for mini computer hardware, spares, transportation, etc.) is so overwhelming, that the other factors cannot be noticed. Even assuming price reductions due to the volume involved, to 10% of the estimated per-system cost, the initial investment would be

$$828 \times \$7500 + \frac{685,000}{828} + .032 \times .50 \times \$149,579,000 = \$8,604,000$$

The operating costs are estimated at $5,000/year per system or $4,140,000. By 1985, the operating costs will be 30% of 1912 systems expected to be in existence then x $5,000 or $2,868,000.

4.5.3 VM Systems

The development costs for a VMM have been estimated variously from $1 million to $3 to $4 million. These are believed to be too high. A reasonable estimate for a larger system is approximately $500,000. The per-system hardware modifications to support a VMM are estimated to be on the order of 10% of the hardware costs. Finally, the overhead of such systems is expected to be on the order of 15%. Using these data, the initial cost of creating a VMM is the initial development cost (e.g. $500,000 per machine type), and the cost of hardware modifications for the VMM (10% of the machine base costs). Since we have indicated that VMM are logical substitutes for dedicated processors, the data from Table 4-13(a) and 4-13(b) is used as the basis for estimating the costs associated with VMM.

If we assume no more than 4 VMM types would be necessary to cover the bulk of the systems; the initial costs are;

$2,000,000	(for 4 VMM's)
$1,944,000	(for hardware mods)
$3,944,000	(total initial costs)

Annual costs for 1980 would be

$$.15 \times 1.075 \times .13 \times \$149,579,000 = \$3,135,549/\text{year}$$

For 1985, with more systems, but presumably no more developments, the costs are:

$$.15 \times 1.075 \times .23 \times \$172,807,000 = 6.408,000/\text{year}$$

4.5.4 Certifiable Systems

The development costs for certifiable systems are on the order of 10 million. The additional cost of hardware to support the development on any given system is on the order of 10%. Finally the operating overhead costs are equally expected to be on the order of 5%.

The initial costs are expected to be on the order of $3,000,000 plus 10% of the hardware base cost.

Initial Development Costs:	$3,000,000
Hardware Modifications:	5,680,000
	$8,680,000

The annual costs for 1980 would be:

.05 x 1.1 x .38 x 149,579,000 = $3,126,000,

where the 38% of the expected system base includes all dedicated processing and system high operation.

For 1985, the costs are

.05 x 1.1 x .58 x $172,807,000 = $5,513,000.

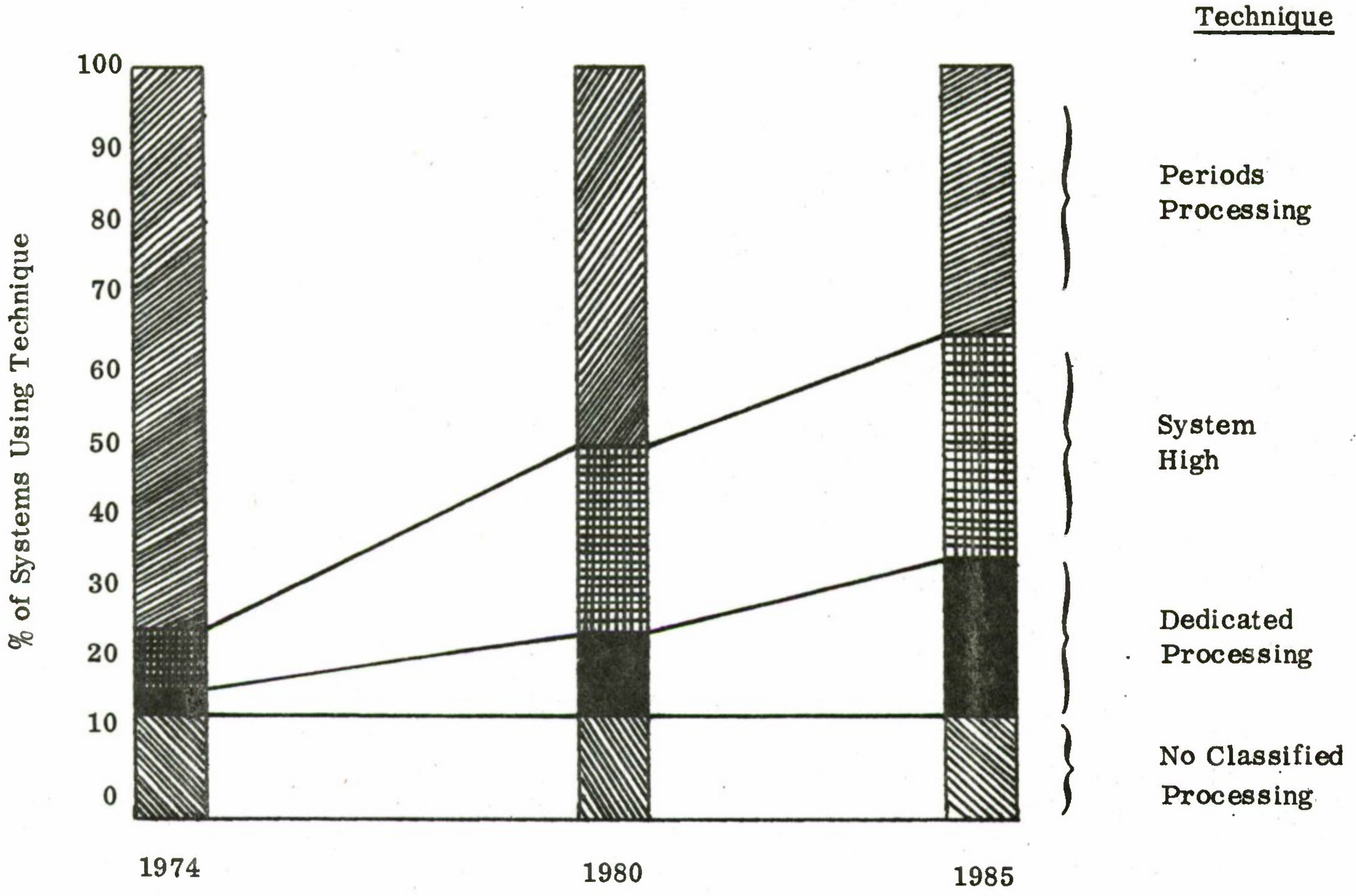


Figure 4-7

Expected Trends in Use of
Security Problem Avoidance Techniques

1974 - 1985

4.6 SUMMARY

Summary data is presented in Table 4-16 and Figures 4-8 and 4-9 From these data a number of conclusions can be drawn.

1. The cumulative costs of avoiding security problems are expected to reach approximately $85,000,000 by 1985. Cumulative costs assuming the availability of VMM or Certified Systems would be expected to reach approximately $70,000.000 by 1985. The bulk of the effect of VMM or Certified Systems would be expected to occur in the period 1980-1985.

2. The Job Stream Separator program has mostly negative impact on computer security costs and should not be pursued.[1]

3. Either VMM or Certifiable Systems would have a significant impact on reducing costs of computer security avoidance techniques. Although the cumulative projected costs for certifiable systems is 2 to 3 million dollars higher than the VMM only costs, it must be kept in mind that the certifiable systems approach can be applied to 40-60% of the systems, while the VMM approach covers from 13 to 23% of the problem. Certifiable systems also permit satisfying "mission essential" requirements that are predicated on information sharing.

[1] Other studies (SCH75) show that even this alternative is cost effective even if only applied to a few WWMCCS sites. This discrepancy is not so much a reflection that the other estimates are many as they are a reflection of the highly conservative (possibly to the point of unrealistically low) estimate of the cost of avoidance are used in this study due to the lack of definitive data to support what might well be more "reasonable" costs.

		Cum.
74	3.209	3.209
75	4.484	7.693
76	5.760	13.453
77	7.036	20.489
78	8.31	28.799
79	9.587	38.38
80	10.868	49.24
81	11.638	60.88
82	12.410	73.28
83	13.181	86.46
84	13.953	100.41
85	13.005	113.42

		Cum.
74	3.209	3.209
75	3.85	7.061
76	4.49	11.55
77	5.14	16.69
78	5.78	22.47
79	6.43	28.90
80	7.07	35.97
81	7.96	43.93
82	8.86	52.79
83	9.75	62.54
84	10.65	73.19
85	11.54	84.73

VMM

		Cum.
74	3.209	
75	3.696	6.90
76	4.184	11.08
77	4.671	15.75
78	5.159	20.92
79	5.65	26.57
80	6.134	32.70
81	6.668	39.36
82	7.203	46.56
83	7.737	54.3
84	8.272	62.57
85	8.018	70.59

Certified Systems

		Cum.
74	3.209	
75	3.828	7.04
76	4.45	11.49
77	5.07	16.56
78	5.69	22.25
79	6.30	28.55
80	6.924	35.47
81	7.269	42.74
82	7.615	50.36
83	7.960	58.32
84	8.306	66.63
85	6.916	73.54

Table 4-16. Summary of Expected Annual and Cumulative Costs For Different Development Strategies

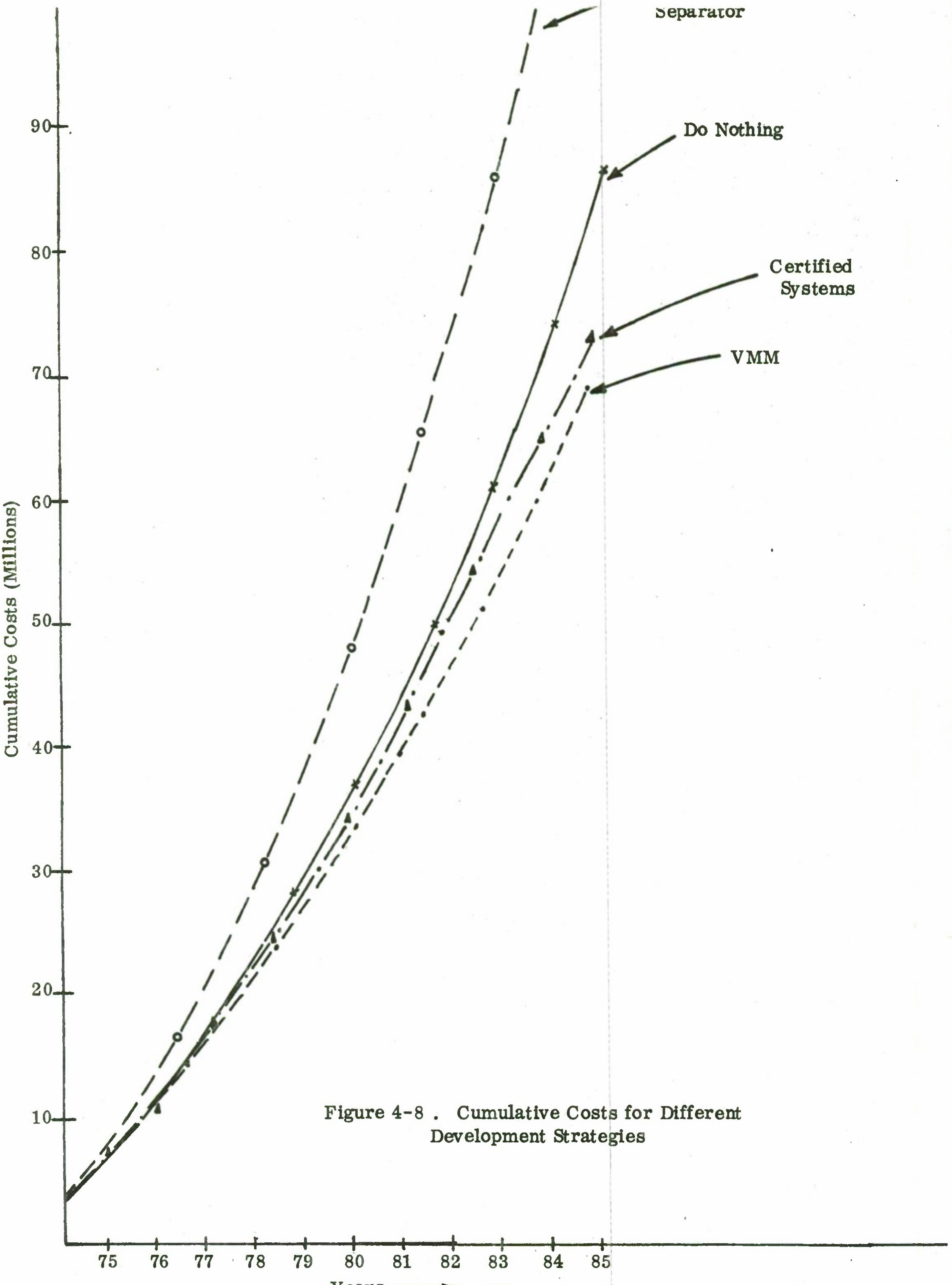


Figure 4-8 . Cumulative Costs for Different Development Strategies

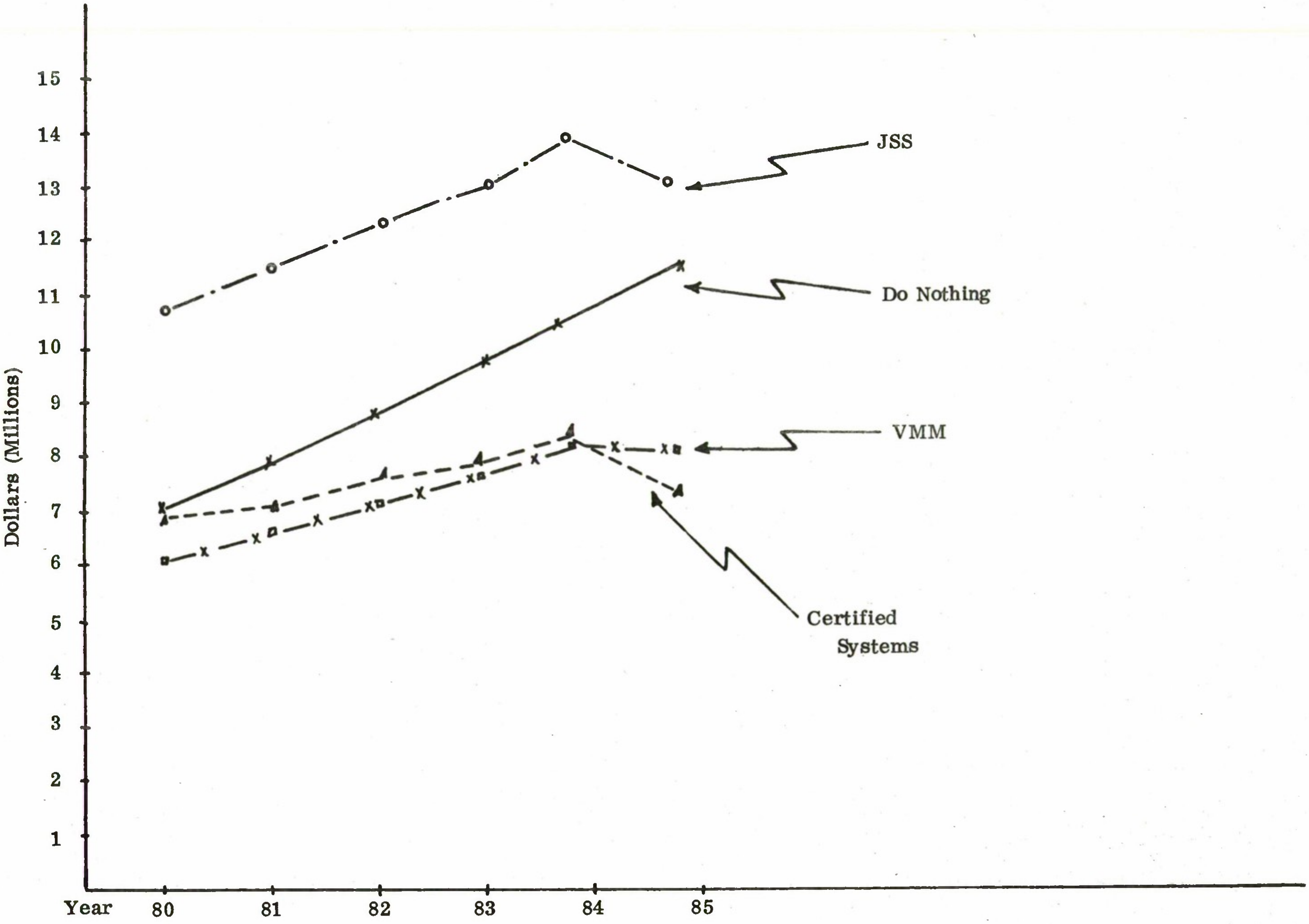


Figure 4-9 . Expected 5 Year Annual Costs of Various Computer Security Development Policies

5. CRITICAL ASSUMPTIONS

5.1 INTRODUCTION

Studies of this kind are replete with assumptions regarding how data processing is utilized, the numbers of systems involved, etc. It is recognized that with better data, the numbers would be expected to change. As a guide to the reader who wishes to make use of his own data for any of the computations in this report, the key assumptions made are summarized in this section. They have been noted in the body of the report as well.

5.2 ASSUMPTIONS

A. The distribution of the number of SMC and GMC systems in each purchase price category is in proportion to the totals 923/1349 for GMC systems and 426/1349 for SMC systems.

B. The average purchase price for USAF systems in each purchase price category is proportional to the data for Government-wide systems.

C. That the estimated % of USAF installations currently using a particular security problem avoidance technique predominently is as shown in Figure 4-5.

D. The annual 'rental' for leased systems is the 'purchase price'/4 and the annual 'rental' for owned systems is the 'purchase price'/7.

E. The number of owned and leased systems in the USAF is proportional to the number of owned and leased CPU's.

F. The number of USAF system installations is approximately 260.

G. The trends to on-line and real-time systems will change the estimated % distribution of use of avoidance techniques for 1980 and 1985 to that shown in Table 4-12.

H. Twenty-five percent is the average fraction of over-capacity due to the security avoidance technique of dedicated processing.

I. Replacement personnel have existing clearances in proportion to those that exist among the personnel in the installation as a whole.

J. Reduction in effective utilization of systems due to periods processing is equivalent to an increase in the dollar cost of a system even if the system is not fully utilized.

K. The over capacity in systems is planned in general, and reduction of it increases cost (in some way).

L. In assessing the impact of possible development paths, it was assumed that JSS would be primarily an alternative to periods processing, VM's would be primarily an alternative to dedicated processors, and certified systems would be primarily an alternative to both dedicated processors and systems high operations. While certified systems could also be alternative to periods processing, none of the cost computations took this into account.

M. No attempt was made to factor in costs associated with secure communications, physical site preparation, lost opportunity costs, and the like. This is in part because there is no easy way to allocate such costs, nor are they known in the same terms of reference as used in this study.

N. Linear extrapolation from 1974 problem avoidance costs to 1980 projected costs for the various strategic alternatives doesn't introduce any significant error.

5.3 CAUTIONS

This study only considers selected costs — those easily estimated from the macroscopic data on the number of systems of various types found in the Inventory of Automatic Data Processing Equipment. Many other very real costs such as those associated with secured communication or physical protection of terminals connected to classified systems have not been considered. Neither has there been any attempt to quantify reduced effectiveness of installations and systems because of the need to employ one or more of the avoidance techniques noted above.

An individual with better data could undoubtedly produce a better study than this. However, in spite of the very obvious limitations of the data and the heavy use of estimated distributions, it is believed that the figures indicate that present security practices have measurable costs, and that these can be greatly improved using modern technology.

REFERENCES

(AND 72) "Computer Security Technology Planning Study," Electronic Systems Division TR-73-51, Vol I, II, Anderson, J. P., October, 1972

(ATT 76) "Penetrating an Operating System: A Study of VM/370 Integrity," Attanasio, C. R., Markstein, P. W., Phillips, R. J., IBM Systems Journal, No. 1, 1976

(BUR 74) "Synthesis of a Software Security System," MITRE Technical Paper-154, Burke, E. L., 15 August 1974

(CCI 72) "Information Processing/Data Automation Implications of Air Force Command and Control Requirements in the 1980's (CCIP-85), SAMSO/XRS, April 1972

(FIS 74) "Automatic Data Processing Costs in the Defense Department," Institute for Defense Analysis Science & Technology Division, Paper P-1046, Fisher, David A., October 1974

(GOL 75) "The Cost of Privacy," Goldstein, Robert C., Honeywell Information Systems, Inc., Brighton, MA, 1975

(INV 74) "Inventory of Automatic Data Processing Equipment in the United States Government for Fiscal Year 1974," Automated Data & Telecommunications Service, GSA, September 1974

(KNI 66) "Changes In Computer Performance," Knight, Kenneth E., Datamation, September 1966, pp. 40-54

(KNI 68) "Evolving Computer Performance 1963-1967," Knight, Kenneth E., Datamation, January 1968, pp. 31-35

(POP 74) "Verifiable Secure Operating System Software," Popek, G. J. and Kline, C. S.; AFIPS Proceedings, Vol. 44, 1974

(SAD 74) "Support of Air Force Automatic Data Processing Requirements Through the 1980's," Electronic Systems Division, AFSC, L. G. Hanscom Field, June 1974

(SCH 75) "Job Stream Separator System Design," MITRE Technical Report 3022, Vol. 1, Schact, J. M., 6 May 1975

MISSION
OF THE
DIRECTORATE OF COMPUTER SYSTEMS ENGINEERING

The Directorate of Computer Systems Engineering provides ESD with technical services on matters involving computer technology to help ESD system development and acquisition offices exploit computer technology through engineering application to enhance Air Force systems and to develop guidance to minimize R&D and investment costs in the application of computer technology.

The Directorate of Computer Systems Engineering also supports AFSC to insure the transfer of computer technology and information throughout the Command, including maintaining an overview of all matters pertaining to the development, acquisition, and use of computer resources in systems in all Divisions, Centers and Laboratories and providing AFSC with a corporate memory for all problems/solutions and developing recommendations for RDT&E programs and changes in management policies to insure such problems do not reoccur.

Printed by
United States Air Force
Hanscom AFB, Mass. 01731